International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 4 269 - 274

Authentication System using Secret Sharing

Nitesh M. Agrawal
M.E. Student, Department of Electronics and Tele- communication,
Sipna C.O.E.T, S.G.B. Amravati University,
Amravati(Maharashtra State), India.
nitesh11391@gmail.com

Dr. Prashant R. Deshmukh
Professor, Department of Electronics and Tele-communication,
Amravati(Maharashtra State), India
pr_deshmukh@yahoo.com

***Abstract*—**Security using Authentication system is an important concern in the field of information technology. It is an important thing as per as concern to the ruling of internet over people today. The growth in the usage of internet has increased the demand for fast and accurate user identification and authentication. This New threats, risks and vulnerabilities emphasize the need of a strong authentication system. The cryptography is a secret sharing scheme where a secret data gets divided into number of pieces called shares and not a single share discloses any information about secret data. There are some automated methods to identify and verify the user based on the physiological characteristics. To deal with such methods, there is a technology called biometrics which measures and statistically analyses the biological data. The biometric samples which are stored in the database as a secret are unique for each user so that no one can predict those samples. A biometric authentication system provides automatic authentication of an individual on the basis of unique features or characteristics possessed by an individual. A cover image is fused with secret image; fused image is divided into n shares. k possible shares able to construct secret image. PSNR parameter are used for image quality

The authentication system can be stronger using multiple factors for authentication process. The application like Aadhar Card uses more than one factor for authentication. There is some difficulty with authentication systems such as user privacy considerations in case of multiple biometric features, huge size databases and centralized database which may create security threats.

To address such tribulations, the Authentication System using Secret Sharing is proposed, Secret sharing splits the centralized database across the different locations. This helps in reducing the database size and removal of threats in centralized database. Also user privacy is maintained due to the decentralized database.

Keywords: *Authentication System, biometric features, secret sharing, Image Fusion, PSNR, MATLAB*

*****

1. INTRODUCTION

Increasing concerns over the personal information has increased the interest in computer security. Our daily lives cannot be separated from We can get lots of information we want by powerful search engine, share the articles or photos in blogs, and contact friends by social network the internet. Many people are dependent on computer systems and networks. This dependency has brought many threats to information security. As a result, information security has become an important issue and hence secure mechanisms are required to protect computers and important information against unauthorized access to computer resources. If we do not process or hide our secret information, the information might be stolen by the hackers easily. Thus authenticity of the user becomes major issue in today's internet applications. The authorized access can be provided through the various authentication methods such as providing passwords or keys. But these methods are not more secure as a password can be forgotten or guessed with bruit force attacks, a key may be lost or stolen and both can be shared. The image hiding and watermarking are techniques that can increase the security of the secret information. However, there is a drawback that the information is kept in a single information-carrier. If the information-carrier is lost or destroyed by an attacker, the secret information might disappear. Thus motivated, the secret sharing method might be the better technique that not only increases the security but also has an extremely high opportunity of recovering the secret information completely.

Secret sharingis an algorithm in cryptography. Secret Sharing Schemes (SSS) refers to method for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use on their own. There are circumstances where an action is required to be executed by a group of people. For example, to transfer money from a bank a manager and a clerk need to cooperate. A ballistic missile should only be launched if three officers authorize the action. Schemes that have a group of participants that can recover a secret are known as Secret Sharing Schemes. Secret sharing has been an active research by mathematicians as object of intrinsic interest in their own right, cryptographers as important cryptographic primitives and security engineers as

technique to employ in distributed security applications. There are various kinds of secret sharing schemes like threshold schemes, schemes with general access structure, verifiable secret sharing schemes, proactive secret sharing schemes etc. As per the need of an application the secret sharing scheme should provide the extended capabilities. To achieve this there is a need of multifarious secret sharing schemes. Concept of secret sharing as shown in fig 1.1.

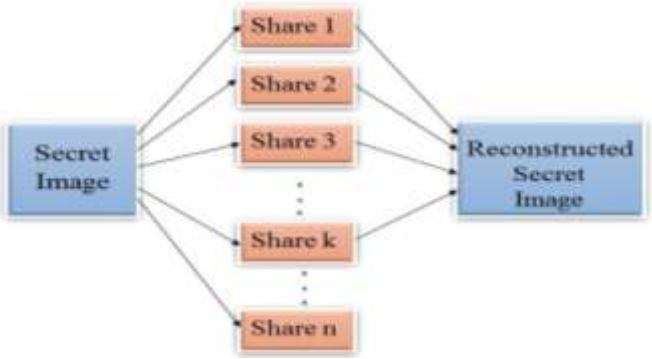

Fig 1.1. Concept of secret sharing

2. PROPOSED WORK

2.1 Objective: -

The main goal of proposed project is to provide secure authentication system which will add following functionalities.

1. To study of Enrolment and Authentication system
2. To design Authentication system using feature extraction and fusion rule also create the shares using secret sharing scheme;
3. To be tested and analyze using Secret Sharing Scheme.
4. Performance evolution parameters of the proposed algorithm to be observed using MATLAB are PSNR, MSE and Correlation factor.

2.2 System Architecture

There are two steps involved in the process of authentication system using secret sharing.

1. Enrolment
2. Authentication

2.2.1. Enrolment Process

In the enrolment process, Images (cover image and secret image) are taken, after taking the images normalization is done on the data to remove the noise. Using the transform domain, the important texture features are extracted from the images and feature vector is generated. Then fusion of the images will be done by using image fusion technique to generate a single image consisting of the secret image as well as the image of the dealer. Hence, secret sharing scheme is applied to split the feature vector into 'n' number of shares. It may be distributed or stored.

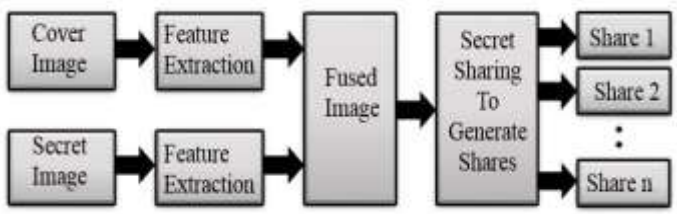

Fig 2.1. User Enrolment Process

2.2.2 Authentication process

In the authentication process, the 'n' number of shares are distributed. Out of that 'k' number of shares are received at receiver. After receiving shares, Images are reconstructed using templet reconstruction. Thus Fused Image is reconstructed. Using the inverse transform domain, the important texture features are extracted from the fused images and feature vector is generated. Hence secured data (secret images) is in form of the images will be obtained.

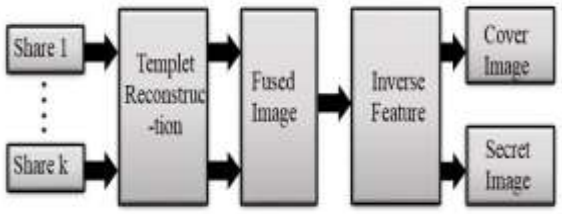

Fig 2.2. User Authentication Process

3. RESULT

This chapter focused on the results of the implemented work on Authentication System using Secret Sharing. In this implemented work to check the different parameters of our scheme we use different types of images like JPEG, PNG, BMP, TIFF etc. that are specially taken as input. On these images various operations are applied. We have developed a conclusion on the basis of parameter explained as shown below and evaluated different parameters for different resolution & different image format.

3.1. Analysis 1: Observing parameter for secret sharing technic

For doing this first choose one image of 256*256 resolution for analysis purposed. We can select this resolution because it is better for analysis as it is convenient for human eye detection. As we have determined better performance parameter. MSE is mean squared error which determines error between the images. In general, minimum error is to be expected but our case is somewhat different. Output image developed during this approach has same as input image,

hence error is zero. Observing the parameter for method as shown in following table 3.1

Table 3.1. Performance parameter for various image format; N=4, K=2

Types of Image	Size of Image	Time to Construct Share	Time to Reconstruct Image	PSNR	Corr.
.JPG	65.8kb	28.47	43.84	Inf	1
.BMP	65 kb	28.34	43.63	Inf	1
.PNG	9.84 kb	27.01	43.51	Inf	1

Table 3.2. value of PSNR of various image format at k = 4,3,2

Method Name	Image Name	Reconstruction			
		S1+S2+S3 +S4+S5	S1+S2+ S3+S4	S1+S2+ S3	S1+S2
A Lossless Secret Image Sharing Scheme on Pixel portioning (By TapasiBhattachrjee [15])	Lena.JPG	Inf	7.49	6.12	5.75
	Child.JPG	Inf	7.43	6.06	5.55
	Flower.bmp	Inf	7.58	5.96	5.45
An Image Secret Sharing Scheme (Implemented)	Lena.JPG	----	Inf	Inf	Inf
	Child.JPG	-----	Inf	Inf	Inf
	Flower.bmp	-----	Inf	Inf	Inf

3.2. Analysis 2: secret sharing on fused Image

For doing this first choose one image as cover image and another one is secret image of various resolution (such as 64*64, 128*128, 256*256 & 512*512) for analysis purposed. We can select various resolution as it is better for analysis performance parameter. Using fusion rule, images are fused then it converted into shares. With the help of required number of shares, we reconstruct secret image as shown below.

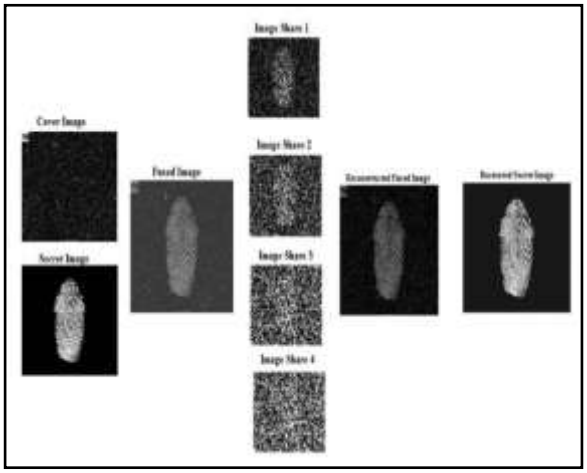

Fig 3.1. secret sharing on fused Image

3.2.1. Observing performance parameter for different image format

For doing this first choose one image as cover image and another one is secret image of resolution 256*256 for analysis purposed. we have determined better performance parameter. PSNR is a quality measurement between the original and a compressed image. Observing parameter for different image format such as .JPG, .TIF, .TIFF, .BMP & .PNG from figure3.2. we observer that PSNR changes from lower to higher range. PSNR should be large because PSNR and MSE inversely proportional to each other. First bar is of .JPG has lowest PSNR & .PNG bar having highest PSNR, hence we conclude that, in this case .PNG image has PSNR than all other image format.

Table 3.3. PSNR at various image format; N=4, K=2

Sr. No.	Types of Images		Size of Images		PSNR
	Cover	Secret	Cover	Secret	
1	.JPG	.JPG	256×256	256×256	38.0453
2	.TIF	.TIF	256×256	256×256	39.7471
3	.TIFF	.TIFF	256×256	256×256	39.7716
4	.BMP	.BMP	256×256	256×256	41.558
5	.PNG	.PNG	256×256	256×256	43.6734

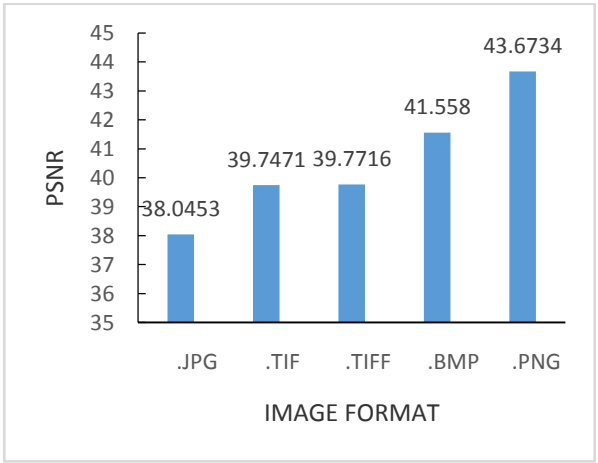

Fig 3.2. PSNR value at various image format

3.2.2. Observing parameter for different image resolution in various format

Most important parameter which reduces the storage requirement of image is nothing but size of image file. Table 3.4. shown below provides all information about this compression for different format. There are different types of images like jpg, png, bmp etc. which we can used. In this case 64*64, 128*128, 256*256 and 512*512 are different resolution of image are used.

By observing figure 3.3, we can say that lower resolution of .JPG image format gives better PSNR. but not necessary that

 ISSN: 2321-8169
269 - 274

every time lower resolution gives PSNR value is better. In case of .BMP image format as resolution is increase from low to high, thus the PSNR are also increases. For higher resolution PSNR is also better. In case of .PNG image format as resolution is increase from low to high, thus the PSNR are also increases. For higher resolution PSNR is also better, as similar to .BMP image format. As in the case of .PNG & .BMP image format image compression ratio is better for higher resolution but in the case of .JPG image format PSNR is better for lower resolution After analysis we have derive this table, depending on table we can conclude that it has better PSNR and reduces storage requirement.

Table 3.4. PSNR &Correlation value for various Image format at various resolution; N=4, K=2

Sr. No.	Types of Images		Size of Images		PSNR	Correlation
	Cover	Secret	Cover	Secret		
1	.JPG	.JPG	64×64	64×64	42.537	0.9992
2	.JPG	.JPG	128×128	128×128	40.3633	0.9989
3	.JPG	.JPG	256×256	256×256	34.399	0.9967
4	.JPG	.JPG	512×512	512×512	34.3168	0.9965
5	.PNG	.PNG	64×64	64×64	38.5448	0.9987
6	.PNG	.PNG	128×128	128×128	40.7791	0.9992
7	.PNG	.PNG	256×256	256×256	43.6734	0.9996
8	.PNG	.PNG	512×512	512×512	44.2308	0.9997
9	.BMP	.BMP	64×64	64×64	34.7395	0.995
10	.BMP	.BMP	128×128	128×128	37.9607	0.9907
11	.BMP	.BMP	256×256	256×256	41.558	0.999
12	.BMP	.BMP	512×512	512×512	44.7253	0.9995

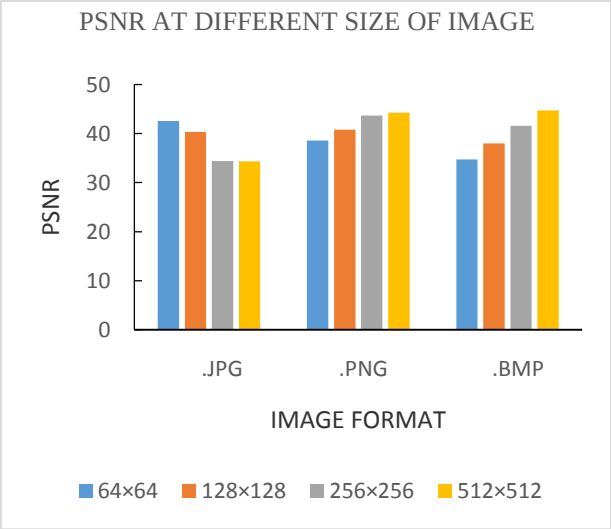

Fig 3.3. PSNR of various image at various resolution.

Observing correlation for different image format at various resolution

For correlation factor, it also same case as that of PSNR in which it compares the two images, provides the information that how much our output image changes with respect input image. By observing fig. 3.4. we can describe another performance parameter correlation. The correlation value of different images at various resolution as shown in table 3.4. In .JPG image format as PSNR is better at lower resolution, thus correlation is also better. At lower resolution in .PNG image format as PSNR is better for 128*128 &256*256 resolution, thus correlation is also better at this resolution. In .BMP image format as PSNR is better for 512*512 resolution, thus correlation is also better.

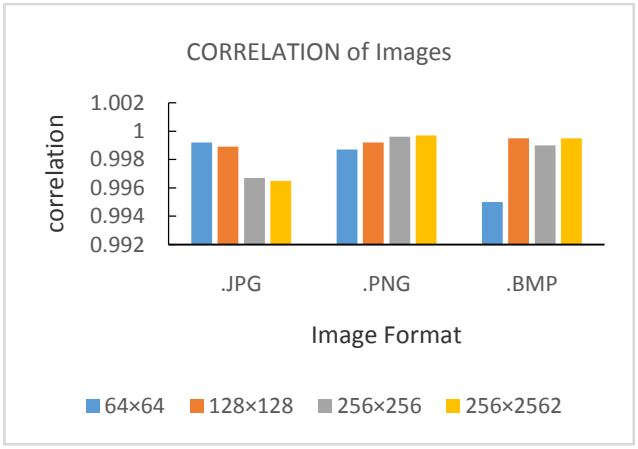

Fig 3.4. Correlation of various resolution.

3.3Analysis 3: proposed work using Excel

3.3.1. secret sharing using Excel file

we are performed the secret sharing scheme on secret image, where a secret image is divided into 'n' parts, giving each participant its own unique part, where 'k' parts or all of them are needed in order to reconstruct the secret image. If this shares are stored into various image format or rotating shares, then shares losses their information. Thus secret image is not constructed. Now we use excel file in secret sharing scheme. Shares are generated by secret sharing scheme are stored in different sheet of same Excel file, thus there is no loss of information. Using various sheet of excel file we reconstruct secret image Fig 3.5. represents following steps

1. we create one excel file.
2. Excel file get divided into 4 shares.
3. The 4 shares are stored into 4 sheet of same excel file.
4. Using 2 sheets of same file we reconstructed original excel file.

By observing Table 3.5. we conclude that, PSNR is infinite and correlation is 1. If correlation factor is 1 then we can say that input file exactly resembles to output file.

Table 3.5. Parameter of secret sharing scheme.

Type of File	No of Shares	Time to construct Share	No of shares Required	Time to reconstruct File	PSNR	CORR.
.xlsx	4	0.47 sec	2	10.56 sec	Inf	1

Fig 3.5. secret sharing using excel file

3.3.2. observing performance parameter using Excel file

In our project we are performed the secret sharing scheme on fused image, as fused image is made up by cover image and secret image. The secret sharing process convert fused image into 'n' number of shares, giving each participant its own unique share, where 'k' shares or all of them are needed in order to reconstruct the secret image. If this shares are stored into image format or rotate, then shares loss their information. Thus secret image is not reconstructed.

Now we used concept of excel file in our project. The Shares of fused image are formed by secret sharing scheme are stored in different sheet of same Excel file. Each share required its separate sheet. as result we can protect shares information from being lost. Using various sheets of same excel file, we reconstruct the fused image. Now secret image is obtained from Fused image. Following fig 3.6.12 represent proposed work using excel file.

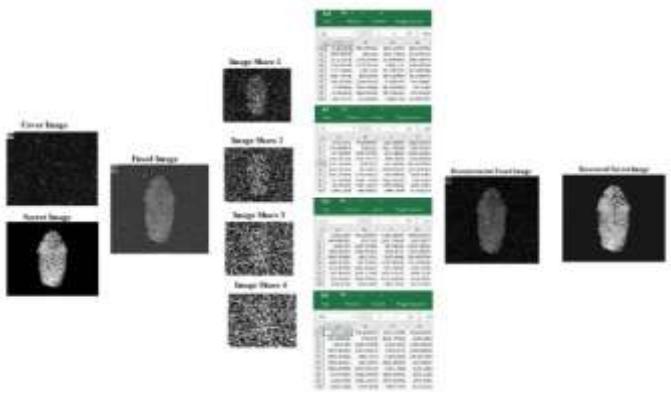

Fig 3.6. Proposed work using Excel file

Table 3.6. shown below provides all information about performance parameter of image resolution of .JPG format. In this case 64*64, 128*128, 256*256 and 512*512 are different resolution of image are used.By observing figure 3.7., we can say that lower resolution of .JPG image format gives better PSNR. As PSNR is better at lower resolution image format, thus Correlation is better for lower resolution.

Table 3.6. Performance Parameter using Excel File, N=4

Sr. No.	Types Images		Size of Images		Share Format	PSNR	Corr.
	Cover	Secret	Cover	Secret			
1	.JPG	.JPG	64×64	64×64	.xlsx	42.537	0.9992
2	.JPG	.JPG	128×128	128×128	.xlsx	40.3633	0.9989
3	.JPG	.JPG	256×256	256×256	.xlsx	34.399	0.9967
4	.JPG	.JPG	512×512	512×512	.xlsx	34.3168	0.9965

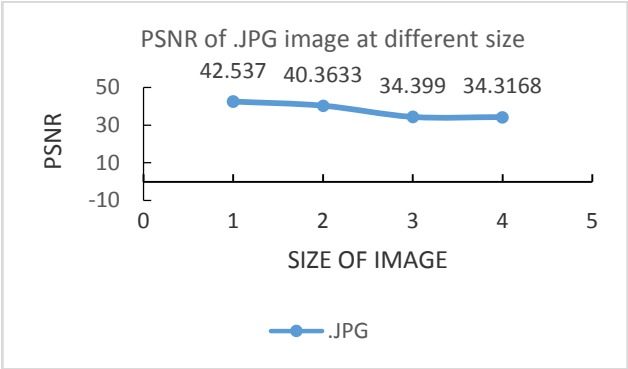

Fig 3.7.value of PSNR Using Excel file

Here we analyses processing time, while comparing for different resolution it differs, simple because the higher resolution has more number of pixel, it takes more time to execute.

4. CONCLUSION

- As per our objectives using MATLAB get impressive speed of operation increased.
- A method of image fusion Stationary Wavelet Transform (SWT) is proposed, we evaluate the Performance results of our proposed method using the PSNR values and found that our proposed fusion method provides good results.
- All shares and reconstruct secret image has the same size with the original secret image
- Shares of Image significantly reduce the memory requirements for the storage.
- We also show that proposed method provides better PSNR value, which gives more perfect output image.
- Our implemented scheme satisfied the security and accuracy condition required by any secret sharing scheme.
- The proposed scheme provides high security as original secret image is fused with cover image then fused image is divided into shares. If attackers are aware it is not possible to reconstruct original secret image.

5. REFERENCES

[1] Adi Shamir, "How to share a secret", *Communication of the ACM*, vol. 22, No. 11, pp. 612-613, 1979.

[2] C. C. Thien, J.C. Lin, "Secret image sharing", Computers Graphics, vol. 26, pp. 765-770, 2002.

[3] SonaliPatil, Prashant Deshmukh, "An Explication of Multifarious Secret Sharing Schemes", *International Journal of Computer Applications*, vol. 46, No. 19, pp. 610, 2012.

[4] Rejeswari Mukesh, V. J. Subashini, "Fingerprint based Authentication System using Threshold Visual Cryptographic Technique", *International Conference on Advances in Engineering, Science and Management*, pp. 16-19, IEEE, 2012.

[5] P. V. Chavan, M. Atique, L. Malik, "Signature based Authentication using Contrast Enhanced Hierarchical Visual Cryptography", *Electrical, Electronics and Computer Science (SCEECS)*, pp. 1-5, IEEE, 2014.

[6] P. S. Revenkar, AnisaAnjum, "Secure Iris Authentication using Visual Cryptography", *International Journal of Computer Science and Information Security*, vol. 3 pp. 217-2215 2010.

[7] M. D. Dhameliya, J. P. Chaudhari, "A Multimodal Biometric Recognition System based on Fusion of Palmprint and Fingerprint", *International Journal of Engineering Trends and Technology*, vol. 4, Issue 5, pp. 1908-191 1, 2013.

[8] P. F. Tsai and Ming—Shi Wang, "An (3, 3) — Visual Secret Sharing Scheme for Hiding 'Three Secret Data", *JCIS*, atlantis-press.com, 2006.

[9] Vinayak Ashok Bharadi, Bhavesh Pandya, BhushanNemade, "Multimodal Biometric Recognition using Iris and Fingerprint — By Texture Feature Extraction using Hybrid Wavelets", *Confluence- The Next Generation Information Technology Summit*, pp. 697-702, IEEE, 2014.

[10] Peng Xinrong, Tian Yangmeng, Wang Jiaqiang, "A survey of Palmprint Feature Extraction Algorithms", International Conference *on Intelligent Systems Design and Engineering Applications*, pp. 57-63, IEEE, 2013

[11] Dr G Raghavendra Rao, P. Devaki – "A Novel Algorithm to Protect the Secret Image through Image Fusion and Verifying the Dealer and the Secret Image'' Fifth International Conference on Signals and Image Processing, pp.77-80, IEEE, 2014

[12] JanhaviSirdeshpande, SonaliPatil- "Amended Biometric Authentication using Secret Sharing."*International Journal of Computer Applications* (0975 – 8887) Volume 98 – pp 29-33, July 2014

[13] Li Bai, S. Biswas, A. Ortiz and D. Dalessandro, "An Image Secret Sharing Method", *International Conference on information Fusion*, pp. I -6, IEEE, 2006.

[14] B Siva Kumar, S Nagaraj – "Discrete and Stationary Wavelet Decomposition for IMAGE Resolution Enhancement", International Journal of Engineering Trends and Technology (IJETT) – Volume4 issue7-July 2013

[15] Tapasibhattacharjee "A lossless Secret Image Sharing Scheme based on Pixel Portioning", *International journal of Electronics communication and computer technology (IJECCT)* Volume 2 issue 1, ISSN 2249-7838,(January 2012)