PROJECT REPORT

ON

SECRET SHARING USING PIXEL GROUPING

Submitted in the fulfillment of the requirement for the award of degree of

Bachelor of Technology
In
Computer Science & Engineering

Submitted by

Nayan Goswami 25300120004
Shruti Singh 25300120013
Swarnadip Guin 25300120014
Souvik Bhattachrjee 25300120019
Isha Maji 25300120029

UNDER THE GUIDANCE OF

Prof. Aritra Bandyopadhyay
Assistant Professor

Department of Computer Science & Engineering
Supreme Knowledge Foundation Group of Institutions

Under

Maulana Abul Kalam Azad University of Technology
Kolkata, West Bengal, India.

MAY, 2024

DECLARATION

We hereby declare that this project report is based on our original work except for citations and quotations which have been duly acknowledged. We also declare that it has not been previously and concurrently submitted for any other degree or award at any University or any other Institution.

NAYAN GOSWAMI
25300120004
Supreme Knowledge Foundation Group of Institutions,
Maulana Abul Kalam Azad University of Technology

SHRUTI SINGH
25300120013
Supreme Knowledge Foundation Group of Institutions,
Maulana Abul Kalam Azad University of Technology

SWARNADIP GUIN
25300120014
Supreme Knowledge Foundation Group of Institutions,
Maulana Abul Kalam Azad University of Technology

SOUVIK BHATTACHARJEE
25300120019
Supreme Knowledge Foundation Group of Institutions,
Maulana Abul Kalam Azad University of Technology

ISHA MAJI
25300120029
Supreme Knowledge Foundation Group of Institutions,
Maulana Abul Kalam Azad University of Technology

Supreme Knowledge Foundation Group of Institutions
1, Khan Road, Mankundu, Hooghly-712139

CERTIFICATE

This is to certify that this project entitled "SECRET SHARING USING PIXEL GROUPING" submitted by NAYAN GOSWAMI(25300120004), SHRUTI SINGH(25300120013), SWARNADIP GUIN(25300120014), SOUVIK BHATTACHARJEE(25300120019), ISHA MAJI(25300120029), students of Computer Science & Engineering Department, Supreme Knowledge Foundation Group of Institutions, Hooghly, West Bengal in the partial fulfilment of the requirement for the award of Bachelors of Technology in Computer Science and Engineering of Maulana Abul Kalam Azad University of Technology, West Bengal, is a record of students' own study carried under my supervision and guidance. This report has not been submitted to any other University or Institution for the award of any degree.

Guide:
Computer Science and Engineering Department
Mr. Aritra Bandyopadhyay
Designation: Assistant Professor

Project Co-ordinator
Computer Science and Engineering Department
Mr. Shibdas Bhattacharya
Designation: Assistant Professor

Department Chair,
CS and IT Studies
Prof. Sayon Ghosh
Designation: Professor

ACKNOWLEDGEMENT

It is a pleasure to thank the many people who made this project work possible for us. It is difficult to overstate my gratitude to my guide, **Prof. Aritra Bandyopadhyay.** With his enthusiasm, his inspiration and his great efforts to explain things simply and clearly, he has helped to make this project work fun for us. Throughout our project work period, he provided encouragement, sound advice, good teaching, good company and lots of good ideas. We would have been lost without him.

We would like to thank our head of the department **Prof. (Dr.) Dhrubasish Sarkar** for providing technical support and computer facilities whenever we needed.

We would like to thank our director **Prof. Dr. Tripti Guin Biswas** for giving us an opportunity to carry out the project work here.

We are indebted to our teachers for providing a stimulating and fun environment in which we learned and grew. We are especially grateful to our family and friends for their help and motivation throughout this work.

Last, but by no means least, we thank our friends for their support and encouragement throughout.

Date:

NAME OF STUDENTS	SIGNATURE OF STUDENTS
NAYAN GOSWAMI	_____
SHRUTI SINGH	_____
SWARNADIP GUIN	_____
SOUVIK BHATTACHARJEE	_____
ISHA MAJI	_____

Place: Mankundu, Hooghly

ABSTRACT

This project is our sincere attempt to make information private and secure during the phase of transmission from sender to receiver. With the rapid development of computer technique and communication network, more and more people and organizations rely on the internet to transmit the important information. However, in recent years, the hackers have intruded many computer and network system to steal or corrupt the important information, which have caused a great loss to the organization and personal profits. Hence information security has become a very important issue in modern society. People generally confuse between privacy and security. Privacy implies private or exclusively belonging to one or a group. And security implies safe transferring of message without any tampering or modifications (wanted or unwanted) by a third person (other than sender or receiver).

Many techniques have been developed to protect the security of information, including cryptography, Steganography, digital watermarking techniques etc. In this project, we have proposed a (n, n) gray level secret sharing method to make it secure for transmission over a medium. The keys are used in the reconstruction of the image. The image can be reconstructed only when all the shares are utilized along with the suitable keys in proper and systematic way. If lesser number of shares is used to reconstruct the image then the image cannot be recovered properly barring the intruders from hacking our data thus ensuring security. Preserving perceivable distortion and prohibiting the imposters from getting any knowledge about our data or information is the main consideration in our thesis.

List of Images and Figures:

Figures:

Using One Pixel:

34. Airplane Original Image
35. Airplane Share1 Construction.
36. Airplane Share2 Construction.
37. Airplane Reconstructed Image.

Three Pixel Algorithm

38. Lena Original Image
39. Lena Share1 Construction.
40. Lena Share2 Construction.
41. Lena Share3 Construction.
42. Lena Share4 Construction.
43. Lena Reconstructed Image.
44. Lady Original Image
45. Lady Share1 Construction.
46. Lady Share2 Construction.
47. Lady Share3 Construction.
48. Lady Share4 Construction.
49. Lady Reconstructed Image.
50. Child Original Image
51. Child Share1 Construction.
52. Child Share2 Construction.
53. Child Share3 Construction.
54. Child Share4 Construction.
55. Child Reconstructed Image.
56. Fly Original Image
57. Fly Share1 Construction.
58. Fly Share2 Construction.
59. Fly Share3 Construction.
60. Fly Share4 Construction.
61. Fly Reconstructed Image.
62. Cameraman Original Image
63. Cameraman Share1 Construction.
64. Cameraman Share2 Construction.
65. Cameraman Share3 Construction.
66. Cameraman Share4 Construction.
67. Cameraman Reconstructed Image.
68. Duck Original Image
69. Duck Share1 Construction.
70. Duck Share2 Construction.

Tables:

ABSTRACT:

This project is our sincere attempt to make information private and secure during the phase of transmission from sender to receiver. With the rapid development of computer technique and communication network, more and more people and organizations rely on the internet to transmit the important information. However, in recent years, the hackers have intruded many computer and network system to steal or corrupt the important information, which have caused a great loss to the organization and personal profits. Hence information security has become a very important issue in modern society. People generally confuse between privacy and security. Privacy implies private or exclusively belonging to one or a group. And security implies safe transferring of message without any tampering or modifications (wanted or unwanted) by a third person (other than sender or receiver).

Many techniques have been developed to protect the security of information, including cryptography, Steganography, digital watermarking techniques etc. In this project, we have proposed a (n, n) gray level secret sharing method to make it secure for transmission over a medium. The keys are used in the reconstruction of the image. The image can be reconstructed only when all the shares are utilized along with the suitable keys in proper and systematic way. If lesser number of shares is used to reconstruct the image then the image cannot be recovered properly barring the intruders from hacking our data thus ensuring security. Preserving perceivable distortion and prohibiting the imposters from getting any knowledge about our data or information is the main consideration in our thesis.

CHAPTER 1

INTRODUCTION:

Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. It is typically carried out by e-mail or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to fool users and exploits the poor usability of current web security technologies.

Phishing is the fastest growing threat in the history of Internet and has gained immense popularity amongst Internet fraudsters and hackers as a simple yet effective way to gain unsolicited access to confidential user information. Using social engineering tactics, fraudsters ensure that the trust relationship established by a company with its customers is exploited to maximum effect. It is for this reason that moving towards stronger identity assurance techniques is the only long term strategy that will maintain the stability of the Internet. Integrity, confidentiality and authentication are fundamental concepts in every marketplace. People and institutions establish trust before conducting business. Traditionally there has been a reliance on physical credentials such as a business license or a letter of intent. In the age of the Internet, communication, transfer of data will only succeed if this ability to pass trust remains consistent. In fact, the future success of a multitude of network communication, data transfer, corporate information, important data monitoring and industrial control and e-commerce ecosystems rests directly upon the continual strengthening of that trust relationship, hence the requirement of network security, message security, user authentication, and key management.

The three security services – confidentiality, authentication and integrity, enable a user to:
_ Communicate securely with a web site – Information which the user then provides cannot be intercepted in transit (confidentiality) or altered without detection (integrity)
_ Verify that the site is actually the company's web site and not an imposter's site (authentication)

In order to create privacy we need to encrypt our message at the sender site and decrypt at the receiver site. The Web presents a unique set of trust issues, which businesses must address at the outset to minimize risk. Consumers submit information and purchase goods or services via the Internet only when they are confident that their personal information, such as credit card numbers and financial data, is secure. So in essence encryption is the process of transforming information to make it unintelligible to all unauthorized parties except the intended recipient and forms the basis of data integrity and privacy which is necessary for e-commerce. What this means is that the whole purpose of encryption is to make sure that the intended recipient is the only one who receives in

intelligible form the information which has been encrypted by converting a plain text into cipher text or code and the receivers site converts it back into plain text.

This is necessary because:

- It makes email servers more secure, compliant, and productive, blocks email threats before they reach our organization.
- Ensure proprietary information that must remain confidential stays where it's safe. Eliminate the need for the ongoing patching and updates required by appliance or software solutions.
- Leverage cloud services to reduce maintenance, conserve bandwidth, and improve the performance of your existing email infrastructure.
- Message Security automatically enforces your email security policies to help assure legal and regulatory compliance for both inbound and outbound email across your organization.
- The services also provides a convenient web console for administration, enabling real-time configuration and policy modifications, monitoring, and alerting as well as reporting for administrators, defining users in the console, or integrate Message Security with our organization directory for easy user synchronization.

The procedures which help us in gaining security are:

CRYPTOGRAPHY:

Cryptography (or cryptology from Greek *kryptos* which means "hidden, secret"; and *gráph*, which means "writing") is the practice and study of hiding information. It refers to the science and art of transforming messages to make them secure and immune to attacks. Modern cryptography intersects the disciplines of mathematics, computer science, and engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

The components involved in cryptography are:

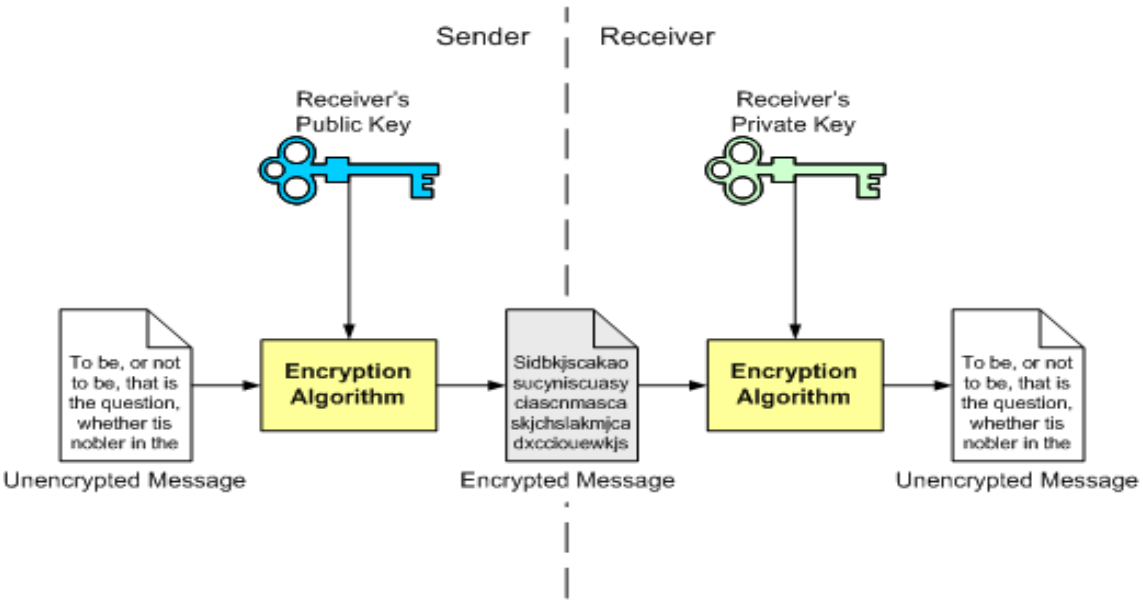


Fig 1: Cryptography components.

The unencrypted message is the Plaintext which is the original message before being transformed. After the message is transformed, it is called cipher text or the encrypted message. An encryption algorithm transforms the plaintext to cipher text; a decryption algorithm transforms the cipher text back to plaintext.

There are two types of cryptography using the data encryption/decryption techniques:

- Symmetric-Key Cryptography: the same key is used by both the parties. The sender uses this key and an encryption algorithm to encrypt the data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.
- Asymmetric-Key Cryptography: It uses a secret key that must be kept from unauthorized users and a public key that can be made public to anyone. Both the public key and the private key are mathematically linked; data encrypted with the public key can be decrypted only by the private key, and data signed with the private key can only be verified with the public key. The public key can be published to anyone. Both keys are unique to the communication session.

SECRET SHARING SCHEME:

A secret sharing scheme, first proposed by Blakley and Shamir independently, is said to implement an access structure when the secret can be reconstructed only if certain sets of players cooperate. A wide range of general approaches for designing secret sharing schemes exists, but most of these techniques result in linear schemes.

Secret sharing 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. More formally, in a secret sharing scheme there are one dealer and n players. The dealer gives a secret to the players, but only when specific conditions are fulfilled. The dealer accomplishes this by giving each player a share in such a way that any group of t (for threshold) or more players can together reconstruct the secret but no group of fewer than t players can. Such a system is called a (t, n)-threshold scheme (sometimes it is written as an (n, t)-threshold scheme). The sharing is performed in such a way that only certain specified subsets of players are able to reconstruct the secret, while smaller subsets have no information about this secret at all (in a strict information theoretic sense).

A secure secret sharing scheme distributes shares so that anyone with fewer than *t* shares has no extra information about the secret than someone with 0 shares. Consider the naive secret sharing scheme in which the secret phrase "password" is divided into the shares "pa------," "--ss----," "----wo--," and "------rd,". A person with 0 shares knows only that the password consists of eight letters. He would have to guess the password from 26^8 = 208 billion possible combinations. A person with one share, however, would have to guess only the six letters, from 26^6 = 308 million combinations, and so on as more persons collude. This system is not a secure secret sharing scheme, because a player with fewer than *t* shares gains significant information about the content of the secret. In a secure scheme, even a player missing only one share should still face 26^8 = 208 billion combinations.

Limitations of secret sharing schemes:

Several secret sharing schemes are said to be information theoretically secure and can be proved to be so, while others give up this unconditional security for improved efficiency while maintaining enough security to be considered as secure as other common cryptographic primitives. For example, they might allow arbitrarily large secrets to be protected by 128-bit shares, since the 2^{128} possible shares are generally considered enough to stymie any conceivable present-day adversary.

Common to all unconditionally secure secret sharing schemes, there are limitations:

- Each share of the secret must be at least as large as the secret itself. This result is based in information theory, but can be understood intuitively. Given t-1 shares, no information whatsoever can be determined about the secret. Thus, the final share must contain as much information as the secret itself.

- All secret sharing schemes use random bits. To distribute a one-bit secret among threshold t people, t-1 random bits are necessary. To distribute a secret of arbitrary length entropy of (t-1)*length is necessary.

Shamir's Secret Sharing

In this scheme, any t out of n shares may be used to recover the secret. The system relies on the idea that you can fit a unique polynomial of degree (t-1) to any set of t points that lie on the polynomial. It takes two points to define a straight line, three points to fully define a quadratic, four points to define a cubic curve, and so on. That is it takes t points to define a polynomial of degree t-1. The method is to create a polynomial of degree t-1 with the secret as the first coefficient and the remaining coefficients picked at random. Next find n points on the curve and give one to each of the players. When at least t out of the n players reveal their points, there is sufficient information to fit a (t-1)th degree polynomial to them, the first coefficient being the secret.

Blakley's scheme:

Two nonparallel lines in the same plane intersect at exactly one point. Three "nonparallel" planes in space intersect at exactly one point. More generally, any n nonparallel n-dimensional hyper planes intersect at a specific point. The secret may be encoded as any single coordinate of the point of intersection. If the secret is encoded using all the coordinates, even if they are random, then an insider (someone in possession of one or more of the n-dimensional hyper planes) gains information about the secret since he knows it must lie on his plane. If an insider can gain any more knowledge about the secret than an outsider can, then the system no longer has information theoretic security. If only one of the n coordinates is used, then the insider knows no more than an outsider (i.e., that the secret must lie on the x-axis for a 2-dimensional system). Each player is given enough information to define a hyper plane; the secret is recovered by calculating the planes' point of intersection and then taking a specified coordinate of that intersection.

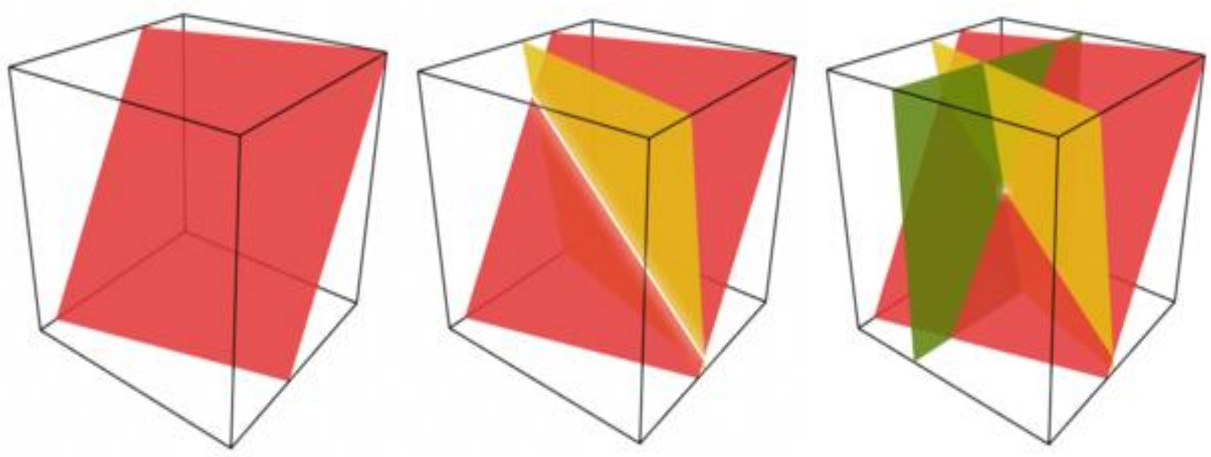


Fig 2: Blakley's Scheme

Blakley's scheme in three dimensions: each share is a plane, and the secret is the point at which three shares intersect. Two shares are insufficient to determine the secret, although they do provide enough information to narrow it down to the line where both planes intersect.

STEGANOGRAPHY:

The word Steganography is of Greek origin and means "concealed writing". With our ever-increasing focus on security, data breaches and fraud, Steganalysis tools, like many security tools, are highly specialized, often with a highly specialized price tag.

It is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message The continuous development of technology has definitely made our job easier and faster but it has also opened the door for many unwanted problems like intruding and hacking of important information being transmitted over the internet. This is why information security has become an indispensable part of our life.

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word Steganography is of Greek origin and means "concealed writing" from the Greek words steganos (στεγανός) meaning "covered or protected", and graphein (γράφειν) meaning "to write". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and Steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible ink between the visible lines of a private letter.

The advantage of Steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, Steganography can be said to protect both messages and communicating parties.

Steganography includes the concealment of information within computer files. In digital Steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

VISUAL CRYPTOGRAPHY:

With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want .To deal with the security problems of secret images, various image secret sharing schemes have been developed.

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement.

Visual cryptography was pioneered by Moni Naor and Adi Shamir in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n-1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

A visual cryptography scheme (VCS) is a special kind of secret sharing scheme in which the secret to share consists of an image and the shares consist of Xeroxed transparencies which are stacked to recover the shared image. In this thesis we have given the theoretical background of Secret Sharing Schemes and the historical development of the subject.

We have, using the secret sharing scheme, first decomposed the pixels of an image and shared it in a particular number of shares, suppose k, then using Shamir's scheme of secret sharing using Lagrange's Interpolation Formula and reconstruction of the image. We have also worked on secret sharing scheme, working on a fixed number of pixels of an image, generating shares from the pixels reading the random matrices values and reconstruction of that image and then finding out using which fixed number of pixels we can better reconstruct the image. Thus the secret sharing scheme used at the sender's site in order to hide data, information to maintain data confidentiality and authentication is put to test in our project.

We are using simple (n, n) gray level image sharing technique. We started our work by utilizing each pixel value of a n x n image which is our secret image .We then generate two (n, n) shares (s1, s2) from the secret image with the help of two 4x4 random matrices(r1,r2) by using various permutation and combination operations. These shares are the scrambled or secret form of the image. The random matrices and the shares taken together are the secret key to the image .The image can be reconstructed only when both the shares are used together and the reverse computation is performed and then the original n x n image is obtained. From the obtained shares the image could be somewhat perceived so we tried to increase the security level and took our efforts one step ahead.

Since the earlier method was slightly less effective as compared to our requirements and security concerns because some portions of the image could be understood even after encryption. Now we took three pixels at a time from the n x n image instead of a single pixel. From the three pixels we generated four n x (n/3) shares (s1,s2,s3,s4) from the secret image with the help of four 8x8 random matrices(r1,r2,r3,r4) by using the same procedure. The reduction in the column size is due to taking of three pixels at a time. The obtained shares were more effective. Now we had four shares and four random matrices as compared to two shares and two random matrices in the earlier version. The image could be reconstructed only when four shares and four random matrices were used together for the purpose of decryption by performing the reverse computational technique to obtain the original n x n image. This method ensures more security as compared to the earlier method since we have eight keys as compared to four in the earlier case. The obtained shares are more scrambled and hence we obtain a better and efficient output since the image cannot be perceived from them individually. The results were satisfactory and so we moved ahead with this concept.

CHAPTER 2

RELATED WORKS:

Berry Schoenmakers et al [1] says a publicly verifiable secret sharing (PVSS) scheme is a verifiable secret sharing scheme with the property that the validity of the shares distributed by the dealer can be verified by any party; hence verification is not limited to the respective participants receiving the shares. We present a new construction for PVSS schemes, which compared to previous solutions by Stadler and later by Fujisaki and Okamoto, achieves improvements both in efficiency and in the type of intractability assumptions. The running time is O (nk), where k is a security parameter, and n is the number of participants, hence essentially optimal. It gives an overview of the refinement in the sharing scheme and the regeneration scheme.

Giorgio Zanin et al [2] defines intricately the mathematical derivations of secret sharing algorithms giving us knowledge about the applications of it in numerous fields.

Helger Lipmaa et al [3] also explains the secret sharing schemes, threshold encryption and multiparty computation explaining in depth how secret sharing occurs.

Pablo Azar et al[4] discussed Shamir's secret sharing protocol. The motivation for this protocol is the desire for individual privacy while computing an aggregate piece of data is what has been told about. It is very well explained how Multi-Party Protocols, Corrupt Players and Corrupt Dealers are coped with preventing them from imposing a threat upon our own message or information.

Ventzislav Stefanov Nikov et al [5] mainly focuses on Cryptography, in particular on unconditionally secure multi-players protocols, and partially on some related areas from Complexity Theory and Coding Theory. This fundamental approach leads first to identification of weaknesses which a considered protocol may possess, identifying possible attacks and strengthening the protocol to resist such attacks, and hence improving its security. Second, the collected knowledge often allows us to improve the efficiency of the protocol with respect to various complexity measures.

Atri Rudra and Scribe: Kanke Gao et al [6] explains the secret sharing schemes: Shamir's secret sharing scheme and a generic secret sharing scheme.

Lin Dong, Min Ku et al [7] proposed a novel (n, n) secret image sharing scheme. The construction of shares is based on matrix multiplication and the revealing is based on addition. The proposed scheme has no pixel expansion and can reconstruct the image precisely.

Daoshan Wang, Lei Zhang, Ning Ma, Xiaobo Li et al [8] discussed about traditional secret sharing schemes involving complex computation. A visual secret sharing decodes the secret without computation, but each shadow is m times as big as the original. It also shows that the (2, n) scheme provides a better contrast and significantly smaller recognized areas than other methods and that the (n, n) scheme gives an exact reconstruction.

Hao-Kuan Tso, Der-Chyuan Lou, Dah-Lih Jeng, and Chao-Lung Chao et al [9] how an image can be reconstructed without loss. They proposed that a (n, n) gray level image sharing method is proposed to solve the problem and only when the n shared images are all gathered, the secret image can be reconstructed without loss.

CHAPTER 3

SECRET SHARING USING PIXEL GROUPING

Generation of shares using Distribution Algorithm:

Step 1: Take an image of size [n X n] and find the matrix form of the image i.e. the pixel values of the image is to be acquired.

Original matrix

	1	2	3	4	
1	149	94	70	71	.....upto [n X n]
2	160	160	161	161	
3	159	160	160	160	
4	159	159	159	159	

Table 1

Step 2: Partition the secret image into k subpixel groups. Repeat the following steps for each k subpixel groups of the secret image.

Step 3: Taking the k pixel values generate the matrix values of the cover images according to the formulae given below:

$$D=a^0 p_i + a^1 * p_{i+1} + a^2 * p_{i+2}$$

where p_i and p_{i+1} are the pixel values of the first and the second cells respectively of the k subpixel group and the value of a ranges from 1 to n, n is the no. of shares to be generated. Here, in this case suppose the k value is 2, therefore the two subpixel values are the values of p_i and p_{i+1} are 149 and 94. So the value of d= 243.

Share=mod (D, 256)

This generates the cover image values or the share values. In this case, the value of Share=243.

Step 3: The mod of D with 256 generates a decimal value. This decimal value is converted into an 8-bit binary value.

Step 4: The 8-bit binary value is partitioned into groups of 3bits, 3bits and remaining 2bits as shown below in Fig 3. The 3values generated from the above partition is converted into decimal number and inserted into the first three cells of each of the cover images.

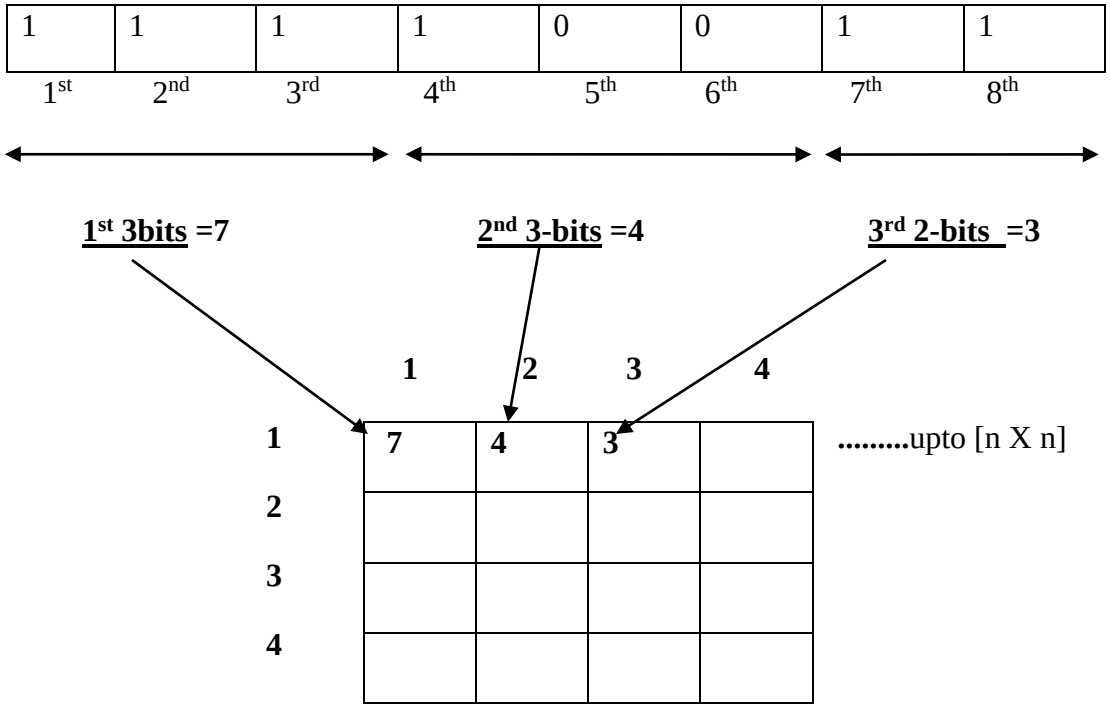


Fig 3

Similarly these values are inserted in each of the n shares i.e. 5 in our case.

Step 5: Repeat the above steps for each subpixel to generate n number of shares.

Construction of cover image and Regeneration using Lagrange's Interpolation Formula:

Step 1: : Take an image of size [n X n] and find the matrix form of the image i.e. the pixel values of the image is to be acquired.

Original matrix

	1	**2**	**3**	**4**	
1	110	24	72	71	**.....**upto [n X n]
2	160	160	161	161	
3	159	160	160	160	
4	159	159	159	159	

Table 2

Step 2: Partition the secret image into k subpixel groups. Repeat the following steps for each k subpixel groups of the secret image.

Step 3: Taking the k pixel values generate the matrix values of the cover images according to the formulae given below:

$$S(a)=a^0 p_i + a^1 * p_{i+1} + a^2 * p_{i+2}$$

where p_i and p_{i+1} are the pixel values of the first and the second cells respectively of the k subpixel group and the value of a ranges from 1 to n, n is the no. of shares to be generated. Suppose in this case k=3, so taking the first 3 pixel values i.e. p_1=110, p_2=24, p_3=72 so using the above formula we can calculate the value of the shares S(1)=206,S(2)=190 and so on till S(5).

Step 4: Using the Lagrange's Interpolation Formulae we reconstruct the share pixel values that we had abstracted using the above formulae. The secret shares s can be reconstructed from every subset of k shares.

Lagrange basis polynomials

$$\ell_j(x) := \prod_{\substack{0\le m\le k \\ m\neq j}} \frac{x-x_m}{x_j-x_m} = \frac{(x-x_0)}{(x_j-x_0)} \cdots \frac{(x-x_{j-1})}{(x_j-x_{j-1})} \frac{(x-x_{j+1})}{(x_j-x_{j+1})} \cdots \frac{(x-x_k)}{(x_j-x_k)}$$

One Pixel Sharing Algorithm:

Step 1:- Take an image of size [n X n] and find the matrix form of the pixel value of the image.

Original matrix

	1	**2**	**3**	**4**	**5**	
1	160	161	161	161	161	**.....**upto [n X n]
2	160	160	161	161	160	
3	159	160	160	160	160	
4	159	159	159	159	159	

Table 3

Step 2:- Take two randomly generated [4 X 4] matrices. Let them be R1 and R2.

R1	**00**	**01**	**10**	**11**
00	47	230	182	33
01	214	168	172	233
10	142	171	6	164
11	8	194	98	251

Table 4

R2	00	01	10	11
00	58	223	34	223
01	61	56	147	204
10	25	73	94	59
11	73	62	103	164

Table 5

Step 3:- Take the first pixel value of the Original matrix and convert it into 8 bits binary value. Increment the location value by 1.

Let the first pixel value be 160. Convert the pixel value into binary form.

Binary of 160 = 10100000 (8 bits)

Step 4:- Divide the 8 bit pixel value into 4 groups of 2 bits each. As shown,

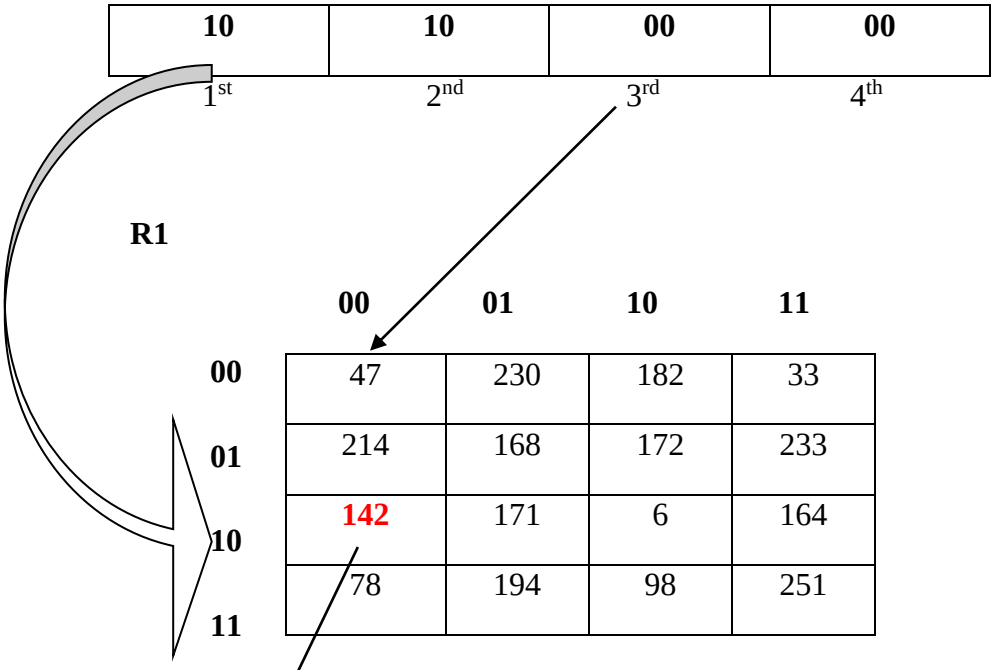
10	**10**	**00**	**00**
1st	2nd	3rd	4th

Table 6

Step 5:- Take the first group as the row index of [4 X 4] random matrix 1 and third group as the column index of [4 X 4] random matrix 1 and find the corresponding value in the matrix for that pixel.

Place the value obtained into the first location of [n X n] share matrix1 and increment the location value by 1.

Fig 4:



This value is put into the <u>first cell (1, 1)</u> of the share1.

Share 1

	1	2	3	4
1	**142**			
2				
3				
4				

…….upto **[**n X n]

Table 7

Similarly, take the second group as the row index of [4 X 4] random matrix2 and fourth group as the column index of [4 X 4] random matrix 2 and find the corresponding value in the matrix for that pixel.

Place the value obtained into the first location of [n X n] share matrix2 and increment the location value by 1.

Step 6:- Continue the Steps 3 to 5, for all the pixel values of the Original image.

Step 7:- Using, all the pixel value of the original image, generate the Share value of both the shares, Share 1 and Share 2. Finally, with the help of Original image we will generate two Share image.

One Pixel Reconstruction Algorithm

Step 1:- Take the first pixel value of Share 1.

Search this value in random matrix **1** and note down the index values**.** ***Row*** index will form ***first*** group and ***Column*** index will form ***third*** group.

Fig 5:

Share 1

	1	**2**	**3**	**4**	
1	**142**	142	142	142	……upto **[**n X n]
2	142	142	142	142	
3	164	142	142	142	
4	164	164	164	164	

R1

	00	**01**	**10**	**11**
00	47	230	182	33
01	214	168	172	233
10	**142**	171	6	164
11	78	194	98	251

The value of the row number i.e. 10 is taken into the 1st cell and the column number i.e. 00 is taken into the 3rd cell as shown below.

10		**00**	
1st	2nd	3rd	4th

Similarly take the first pixel value of Share 2.

Search this value in random matrix 2 and note down the index values. Here Row index will form second group and Column index will form fourth group.

Fig 6:

Share 2

	1	**2**	**3**	**4**	
1	**25**	73	73	73	……upto [n X n]
2	25	25	73	73	
3	204	25	25	25	
4	204	204	204	204	

Table 8

R2

	00	**01**	**10**	**11**
00	58	223	34	223
01	61	56	147	204
10	**25**	73	94	59
11	73	62	103	164

10	**10**	**00**	**00**
1st	2nd	3rd	4th

Convert each of the index values thus obtained into 2bits binary value. Hence we get 4 groups of 2 bits each. As shown above.

Step 2:- Now concatenate the 4 groups' one after the other to get a final binary value of 8 bits.

Final binary value = 10100000 (8 bits).

Step 3:- Convert the 8 bits binary value into decimal form and insert it into the first location of the [256 X 256] reconstructed matrix .Then increment the location value by 1.

Fig 7:

Decimal form of 10100000 (8 bits) = 160.

Reconstructed matrix (Table 9)

	1	**2**	**3**	**4**	**5**	
1	**160**					**.....**upto [n X n]
2						
3						
4						

Do the same for the rest of the pixel values of Share matrices to get final reconstructed matrix of size [n X n].

Step 4:- Using all the share pixel values of the Share 1 and Share 2 generate a reconstructed matrix. As shown, and generate the reconstructed Image.

Final Reconstructed matrix

	1	**2**	**3**	**4**	**5**	
1	160	161	161	161	161	**.....**upto [n X n]
2	160	160	161	161	160	
3	159	160	160	160	160	
4	159	159	159	159	159	

Table 10

Three Pixel Sharing Algorithm

The One Pixel Method generates exceptionally good reconstructed image but the shortcoming is that the shares generated are not as concealing in nature as was the need of the hour. The obtained shares are not very much impressive and the probability of guessing or reconstructing the image from individual shares is higher. Therefore we try the Three Pixel Method.

Step 1:- Take an image of size [n X n] and find the matrix form of the image i.e. the pixel values of the image is to be acquired.

	1	**2**	**3**	**4**	**5**	
1	160	161	161	161	161	**.....**upto [n X n]
2	160	160	161	161	160	
3	159	160	160	160	160	
4	159	159	159	159	159	

Table 11: Original matrix

Step 2:- Take four randomly generated [8 X 8] matrix. Let them be R1, R2, R3 and R4. For e.g. R1 is shown in the fig. below.

RANDOM MATRIX (R1):

	000	**111**	**101**	**110**	**001**	**010**	**011**	**100**
000	44	171	54	121	1	200	112	83
001	243	192	174	216	167	151	136	49
101	243	186	120	22	94	237	167	162
011	186	20	135	181	222	58	239	185
100	176	75	1	72	2	22	190	71
101	103	168	141	159	116	63	239	47
110	224	14	41	183	76	22	148	111
111	139	197	243	66	155	90	55	221

Table 12: Random matrix R1

Similarly, generate random matrices for **R2, R3** and **R4 (keeping in mind that the same value does not appear a number of times else noise is viewed in the output).**

Step 3:- Take the first 3 pixels and convert each one into 8 bits binary value. Concatenate these 8 bits values together to get a 24 bits value. Increment the location value by 3.

Let first three Pixel values be 160, 161 and 161. Convert the pixel values into binary form.

Binary of 160 = 10100000 (8 bits),

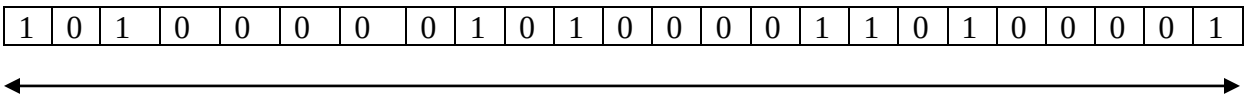
Binary of 161 = 10100001 (8 bits),

Binary of 161 = 10100001 (8 bits),

Concatenate all 8 bits three pixel values to get 24 bit values.

10100000 10100001 10100001

160 161 161



Step 4:- Divide the 24 bit pixel values into 8 groups of 3 bits each.

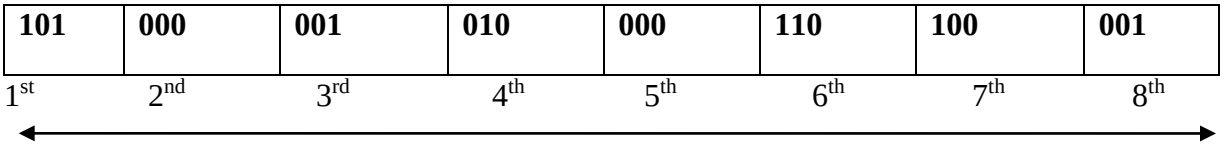
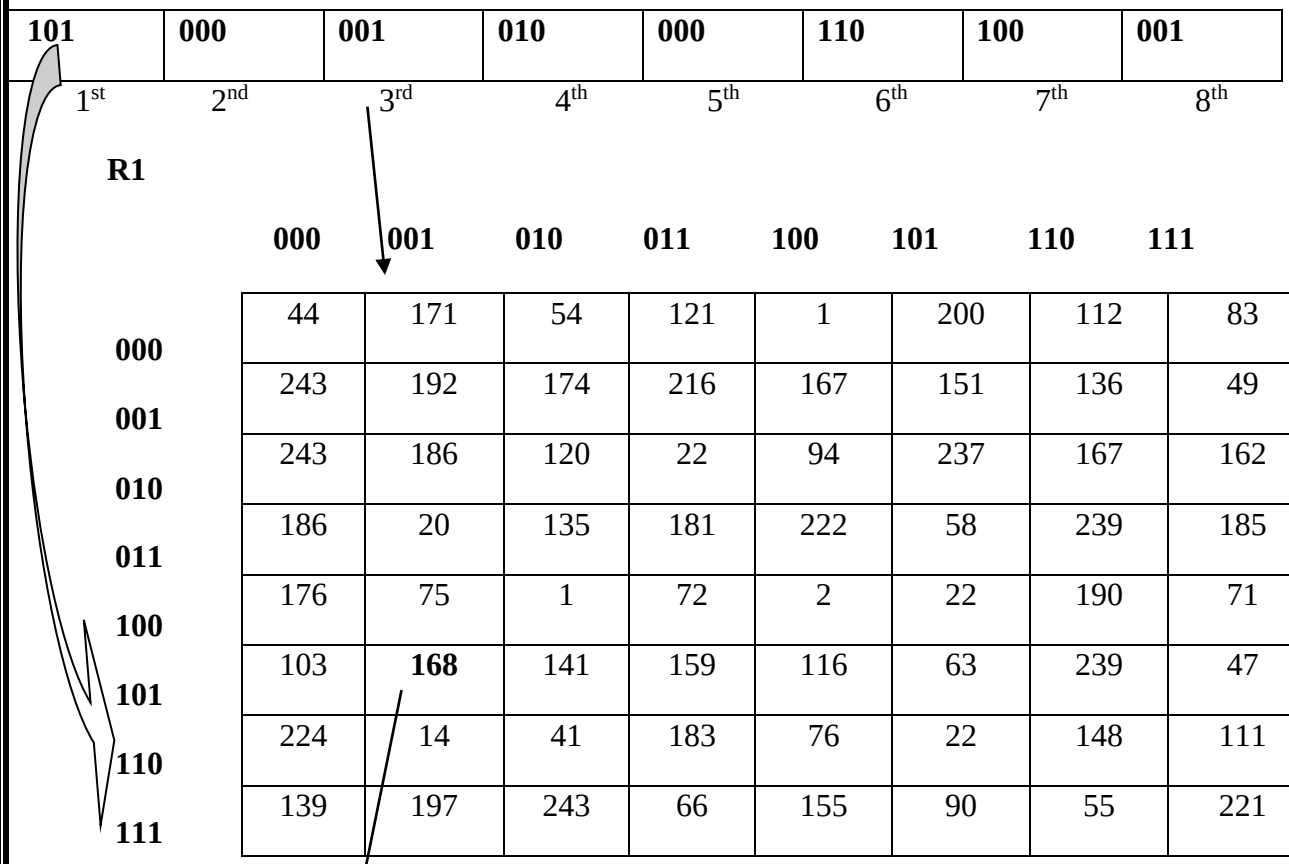


Table 13

Step 5:- Take the ***first*** group as the ***row*** index of [8 X 8] random matrix 1 and ***third*** group as the ***column*** index of [8 X 8] random matrix 1 and find the corresponding value in the random matrix for that pixel.

Place the value obtained into the ***first*** location of [n X n/3] ***share matrix1*** and increment the location value by 1.

Fig 8:



Similarly, take the ***second*** group as the ***row*** index of [8 X 8] random matrix2 and ***fourth*** group as the ***column*** index of [8 X 8] random matrix 2 and find the corresponding value in the random matrix for that pixel.

Place the values obtained into the first location of [n X n/3] ***share matrix 2*** and increment the location value by 1.

Similarly, take the ***fifth*** group as the ***row*** index of [8 X 8] random matrix **3** and ***seventh*** group as the ***column*** index of [8 X 8] random matrix 3 and find the corresponding value in the matrix for that pixel.

Place the value obtained into the first location of [n X n/3] ***share matrix3*** and increment the location value by 1.

Similarly, take the ***sixth*** group as the ***row*** index of [8 X 8] random matrix 4 and ***eighth*** group as the ***column*** index of [8X8] random matrix4 and find the corresponding value in the matrix for that pixel.

Place the value obtained into the first location of [n X n/3] ***share matrix4*** and increment the location value by 1.

Step 6:- Continue the Steps 3 to 5 for all the pixel values of the original image.

Step 7:- Using, all the pixel values of the original image, generate the Share value of all the four shares, Share 1, Share 2, Share 3 and Share 4. Finally, with the help of Original image we will generate four Share images.

Three Pixel Reconstruction Algorithm

Step 1:- Take the first pixel value of ***Share 1.***

Search this value in random matrix 1(R1) and note down the index values. ***Row*** index will form ***first*** group and ***Column*** index will form ***third*** group.

Fig 9:

Share 1

	1	**2**	**3**	**4**
1	**168**	159	71	22
2	168	159	71	72
3	71	168	22	75
4	71	71	72	71

…….upto **[**n X n/3]

R1

	000	**001**	**010**	**011**	**100**	**101**	**110**	**111**
000	44	171	54	121	1	200	112	83
001	243	192	174	216	167	151	136	49
101	243	186	120	22	94	237	167	162
011	186	20	135	181	222	58	239	185
100	176	75	1	72	2	22	190	71
101	103	**168**	141	159	116	63	239	47
110	224	14	41	183	76	22	148	111
111	139	197	243	66	155	90	55	221

101		**001**					
1st	2nd	3rd	4th	5th	6th	7th	8th

Similarly, take the first pixel value of Share **2.**

Search this value in random matrix 2 and note down the index values. Here ***Row*** index will form ***second*** group and ***Column*** index will form ***fourth*** group.

Similarly, take the first pixel value of Share **3.**

Search this value in random matrix 3 and note down the index values. Here ***Row*** index will form ***fifth*** group and ***Column*** index will form ***seventh*** group.

Similarly, take the first pixel value of Share **4.**

Search this value in random matrix 4 and note down the index values. Here ***Row*** index will form ***sixth*** group and ***Column*** index will form ***eighth*** group.

Convert each of the index values thus obtained into 3bits binary value. Hence we get 8 groups of 3 bits each.

101	**000**	**001**	**010**	**000**	**110**	**100**	**001**
1st	2nd	3rd	4th	5th	6th	7th	8th

Step 2:- Now concatenate the 8 groups' one after the other to get a final binary value of 24 bits.

Final binary value = 101000001010000110100001 (24 bits)

Step 3:- Now divide the 24 bits value into 3 groups of 8 bits each.

10100000 / **10100001** / **10100001**

1st 2nd 3rd

Step 4:- Convert the first 8 bits binary value into decimal form and insert it into the first location of the [255 X 255] reconstructed matrix .Then increment the location value by 1.

Convert the second 8 bits binary value into decimal form and insert it into the second location of the [255 X 255] reconstructed matrix .Then increment the location value by 1.

Convert the third 8 bits binary value into decimal form and insert it into the third location of the [255 X 255] reconstructed matrix .Then increment the location value by 1.

Decimal form of 1st 8 bits binary value 10100000 = 160.

Decimal form of 2nd 8 bits binary value 10100001 = 161.

Decimal form of 3rd 8 bits binary value 10100001 = 161.

Reconstructed matrix

	1	**2**	**3**	**4**	**5**	
1	**160**	**161**	**161**			**.....**upto [n X n]
2						
3						
4						

Table 14

Do the same for the rest of the pixel values of Share matrices to get the final reconstructed matrix of size [255 X 255].

Step 4:- Using all the share pixel values of the Share 1 and Share 2 generate a reconstructed matrix. As shown, and generate the reconstructed Image.

Final Reconstructed matrix

	1	**2**	**3**	**4**	**5**	
1	160	161	161	161	161	**.....**upto [n X n/3]
2	160	160	161	161	160	
3	159	160	160	160	160	
4	159	159	159	159	159	

Table 15

CHAPTER 4

Experimental Results

We have worked on Microsoft Windows XP system with a Pentium® Dual Core Processor. We have implemented our algorithm in application software MATLAB (R2007b). In the following pages we display all the results obtained using the One Pixel Sharing Algorithm and Three Pixel Sharing Algorithm.

First we have experimented on the image **lena.jpg** of size [256 X 256]. We have first generated 2 shares of size [256 X 256] from the original image using two different random matrices. These four random matrices are our codebook and is used as a key for encryption purpose. Then we have tried to reconstruct the original image using these shares and their corresponding random matrices. Finally we have calculated the peak signal to noise ratio between the original images and reconstructed.

Similarly, we have experimented on 6 more images. Each image has its own two shares which are also used for the reconstruction of the original image. The Six images used are:

Lady.jpg, Child.jpg, Fly.jpg, Cameraman.jpg, Airplane.jpg, duck.jpg.

However, in order to make our proposal more secure and safe we have changed our approach from One Pixel Sharing Algorithm to Three Pixel Sharing Algorithm.

Then we have experimented on the image **lena.jpg** of size [256 X 256]. Using the Three Pixel Sharing Algorithm, we have first generated 4 different shares of size [255 X 85] using 4 different random matrices. These four random matrices are our codebook and is used as a key for encryption purpose. Then we have tried to reconstruct the original image using these shares and their corresponding random matrices. Finally we have calculated the peak signal to noise ratio between the original images and reconstructed.

Similarly, we have experimented on 4 more images. Each image has its own two shares which are also used for the reconstruction of the original image. The Six images used are:

Lady.jpg, Child.jpg, Fly.jpg, Cameraman.jpg, Airplane.jpg, duck.jpg.

Once the shares are generated we arrange these share and matrix combinations in such a way that until two or more share are gathered together and worked on, no one can reconstruct the original image. Hence, we make various combinations of the share and its corresponding matrix and then send it to various recipients. The main intention over here is that no recipient will have more than one share and matrix combination. This separation of shares ensures security of our secret image.

Experimental Results for One Pixel Sharing Algorithm

Image name: - lena.jpg

Fig 10: Original Image

Share 1 **Share 2**

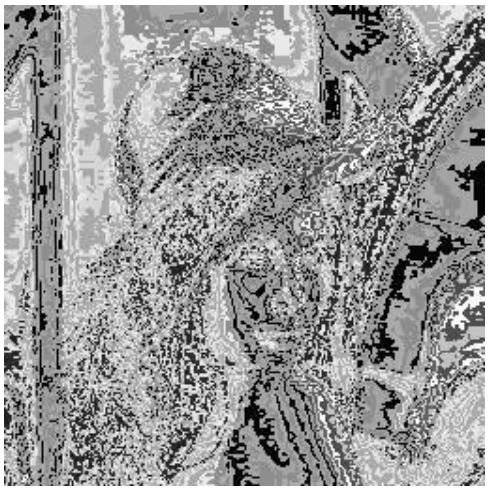


Fig 11

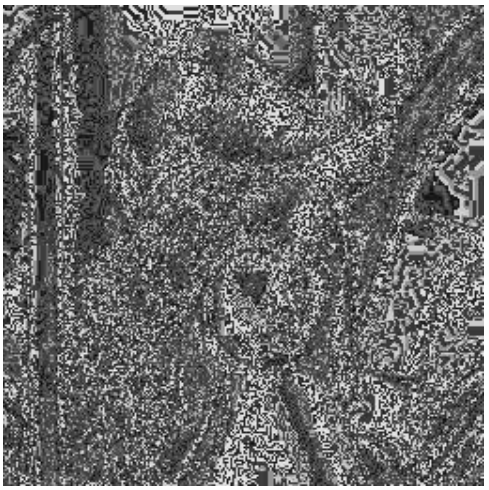


Fig 12

Reconstruction of Original Image using the Share

Share 1

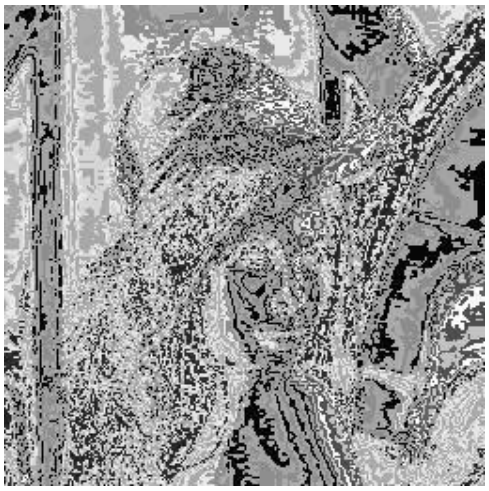


Fig 11

Share 2

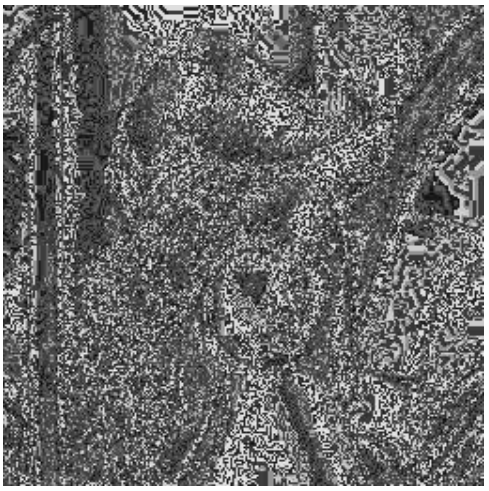


Fig 12

Fig 13: Reconstructed Image

Image name: - lady.jpg

Fig 14: Original Image

Share 1 Share 2

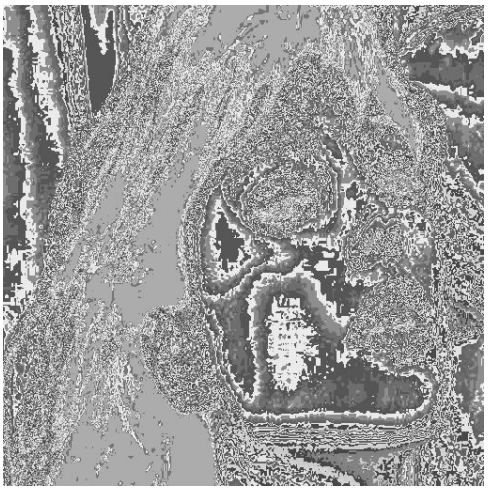


Fig 15

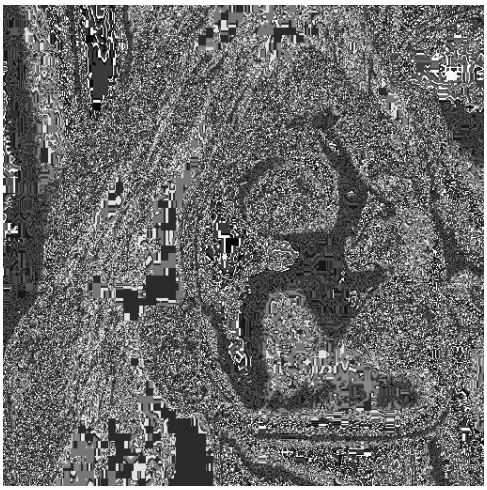


Fig 16

Reconstruction of Original Image using the Share

Share 1

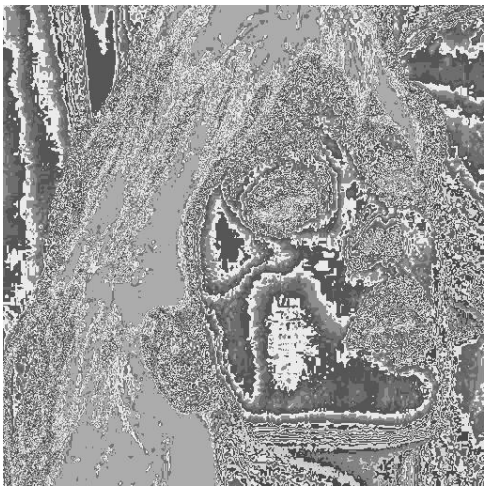


Fig 15

Share 2

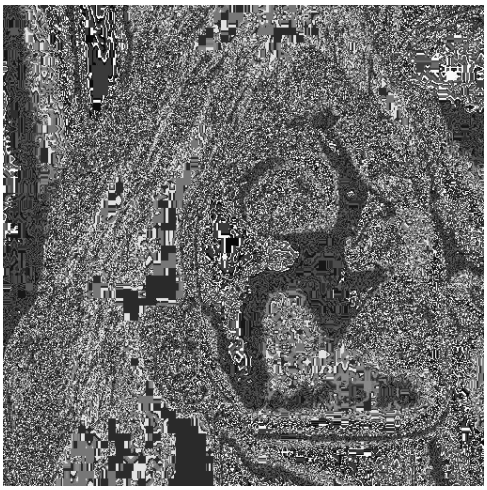


Fig 16

Fig 17 Reconstructed Image

Image name: - child.jpg

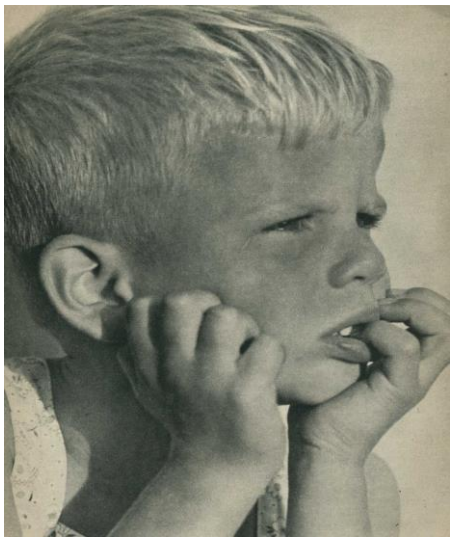


Fig 18: Original Image

Share 1

Share 2

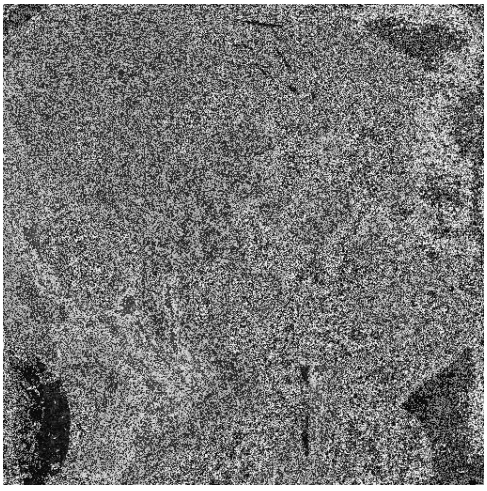


Fig 19

Fig 20

Reconstruction of Original Image using the Share

Share 1

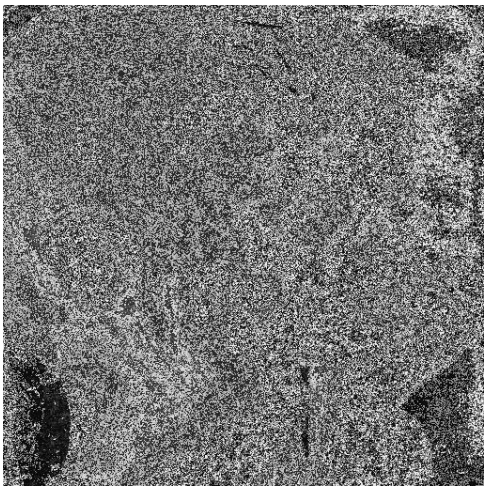


Fig 19

Share 2

Fig 20

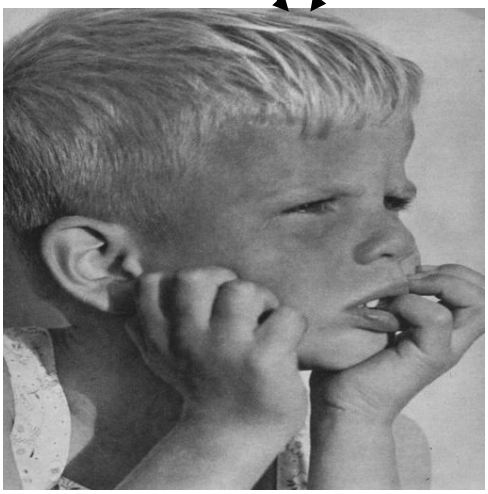


Fig 21: Reconstructed Image

Image name: - fly.jpg

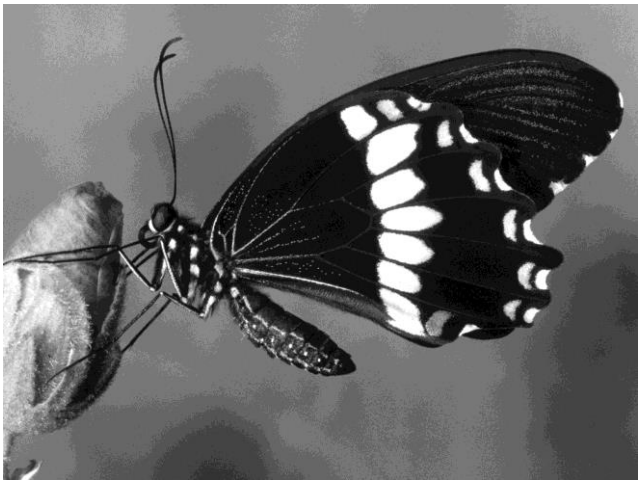


Fig 22: Original Image

Share 1

Share 2

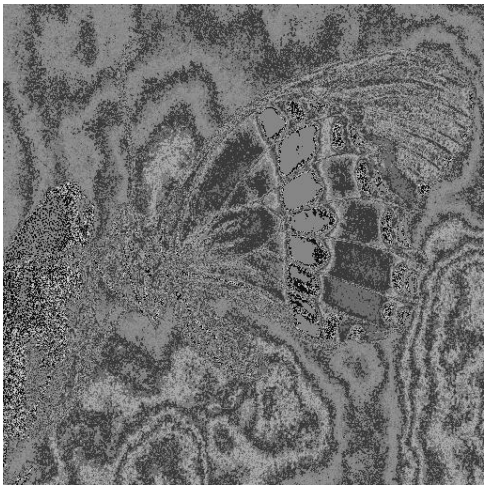


Fig 23

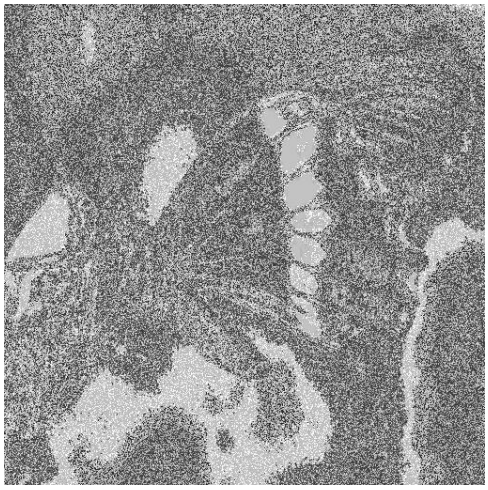


Fig 24

Reconstruction of Original Image using the Share

Share 1

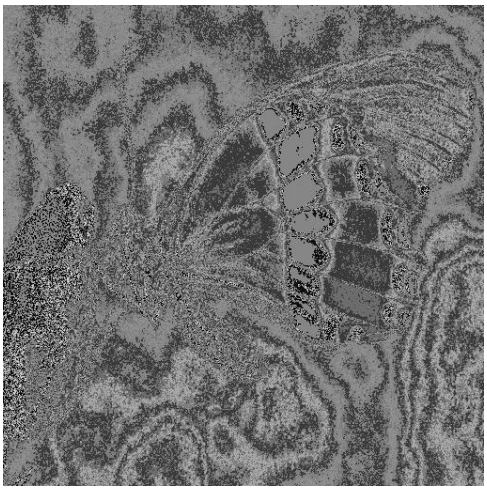


Fig 23

Share 2

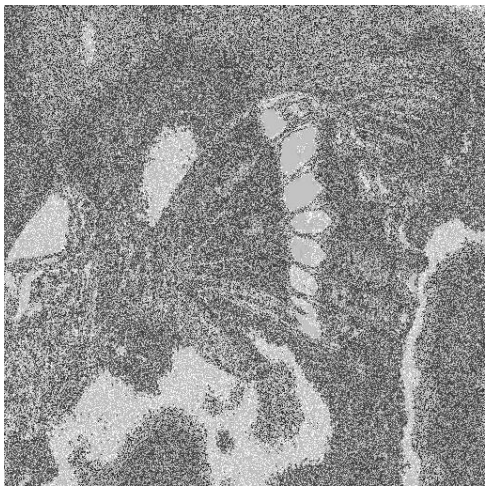


Fig 24

Fig 25: Reconstructed Image

Image name: - cameraman.jpg

Fig 26: Original Image

Share 1

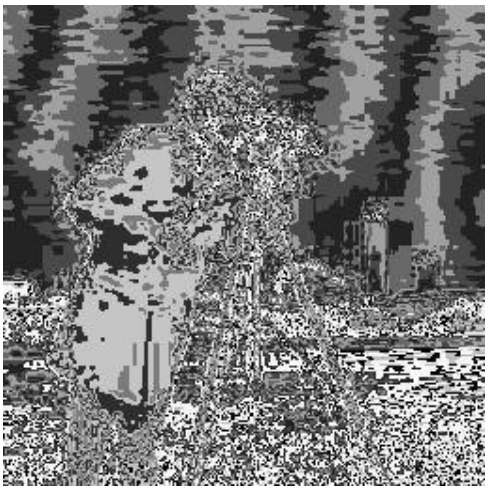


Fig 27

Share 2

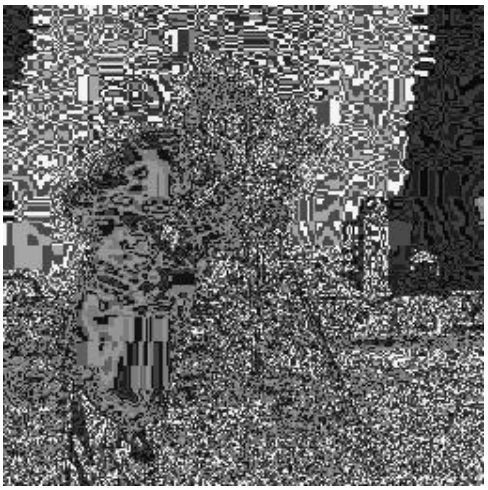


Fig 28

Reconstruction Of Original Image using Two Share Reconstruction Algorithm

Share 1

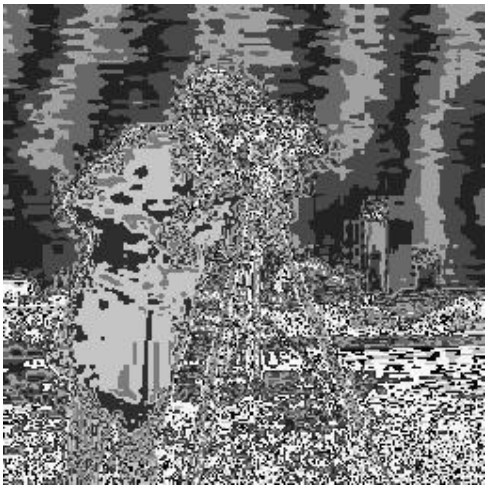


Fig 27

Share 2

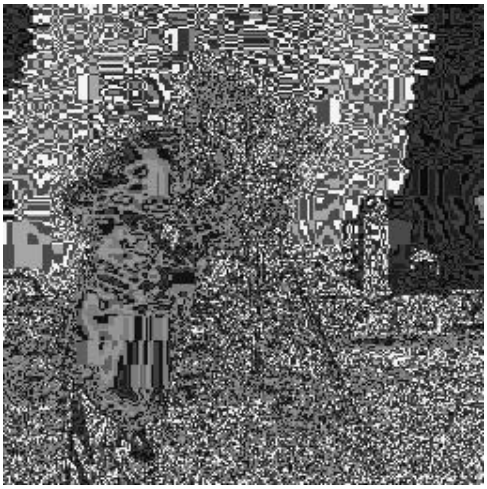


Fig 28

Fig 29 Reconstructed Image

Image name: - duck.jpg

Fig 30: Original Image

Share 1

Share 2

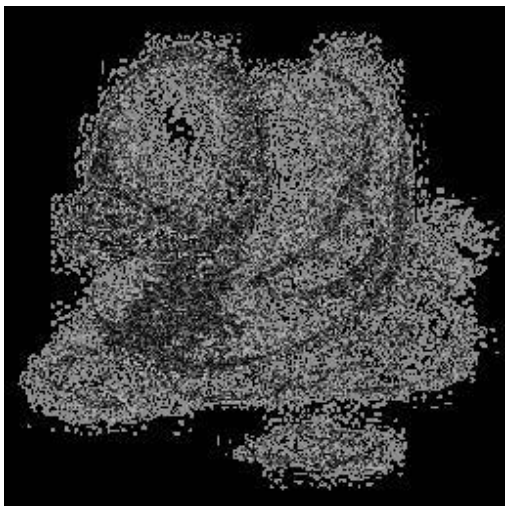


Fig 31

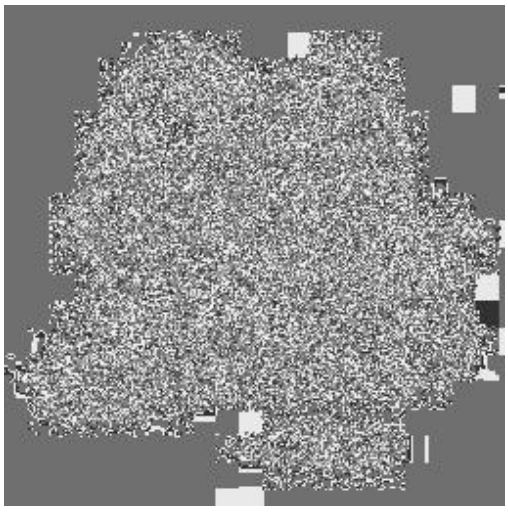


Fig 32

Reconstruction of Original Image using the Share

Share 1

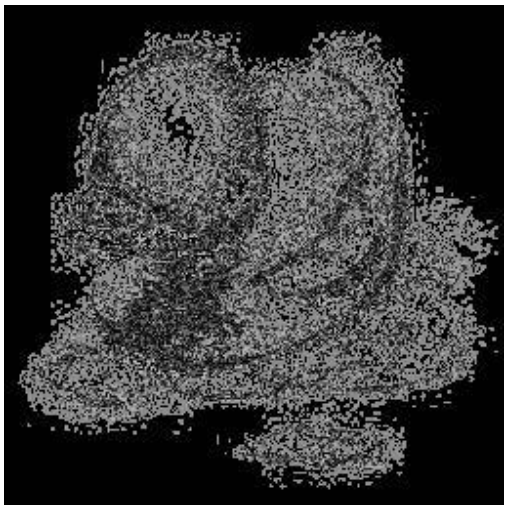


Fig 31

Share 2

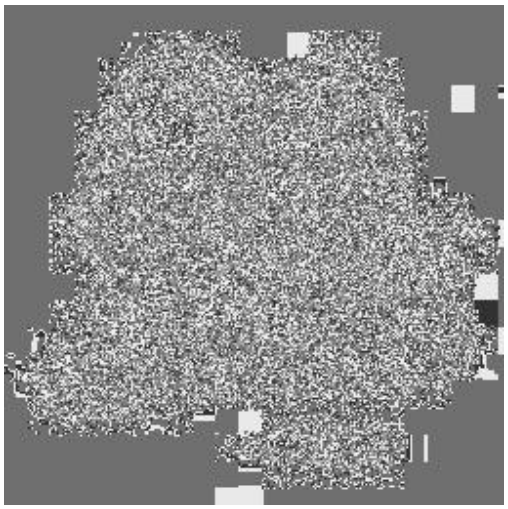


Fig 32

Fig 33: Reconstructed Image

Image name: airplane.jpg

Fig 34: Original Image

Share 1

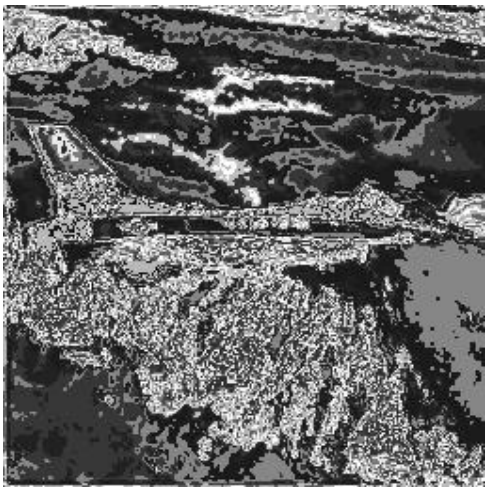


Fig 35

Share 2

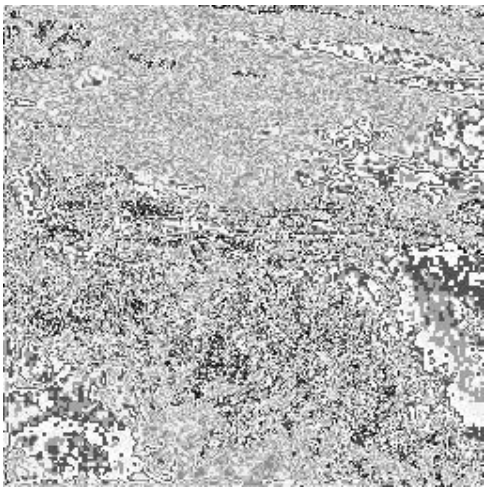


Fig 36

Reconstruction of Original Image using The Share

Share 1

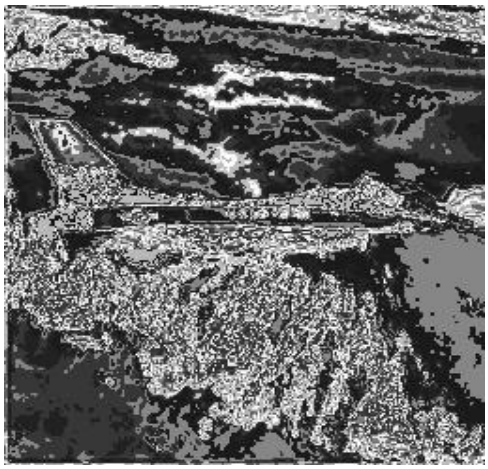


Fig 35

Share 2

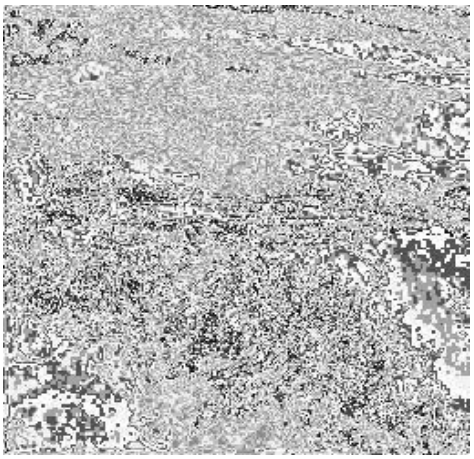


Fig 36

Fig 37: Reconstructed Image

Experimental Results for Three Pixel Sharing Algorithm

Image name: lena.jpg

Fig 38: Original Image

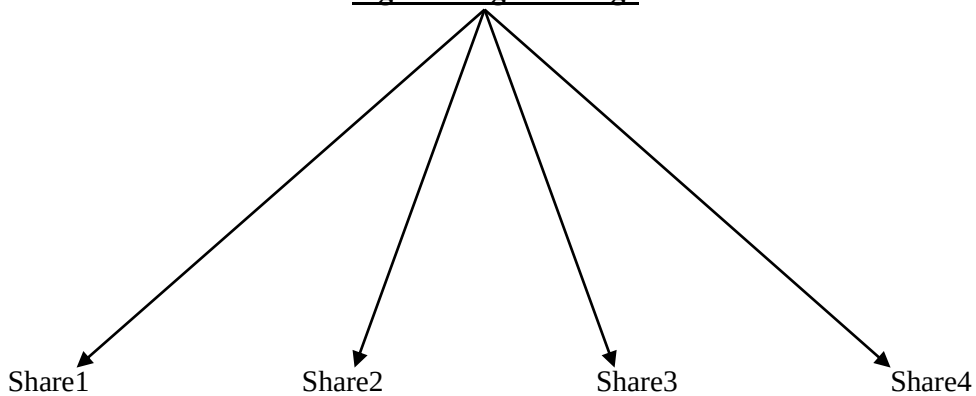


Fig 39

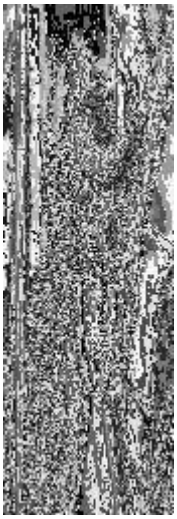


Fig 40

Fig 41

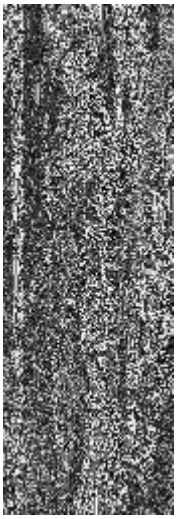
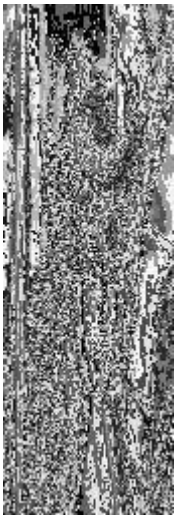


Fig 42

Reconstruction of original image using the shares

Share1 Share2 Share3 Share4



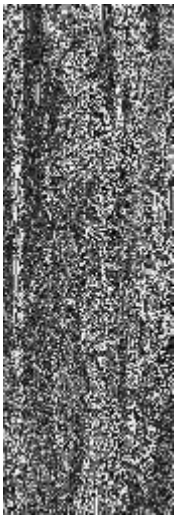


Fig 39 **Fig 40** **Fig 41** **Fig 42**

Fig 43: Reconstructed Image

Image name: lady

Fig 44: Original Image

share1 share 2 share 3 share 4

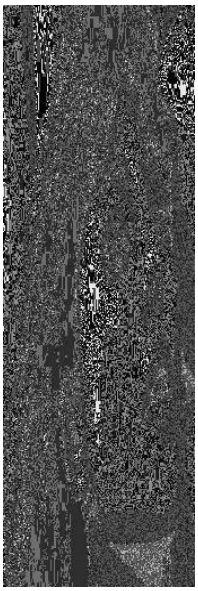


Fig 45

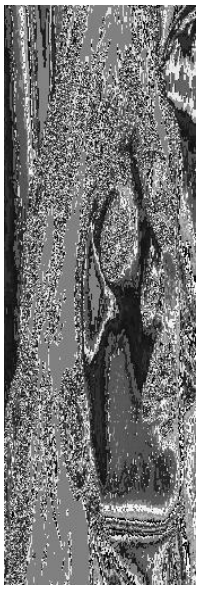


Fig 46

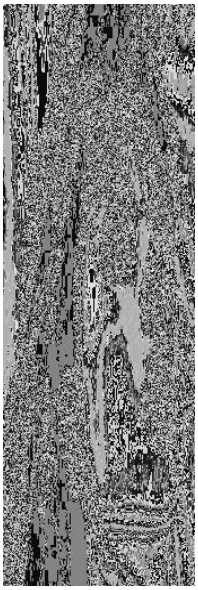


Fig 47

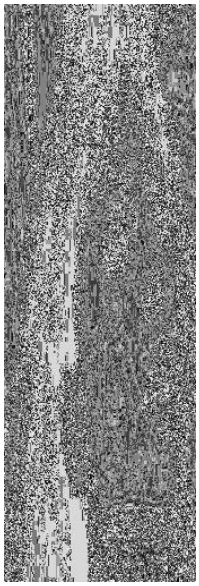


Fig 48

Reconstruction of original image using the shares

Share1 share 2 share 3 share 4

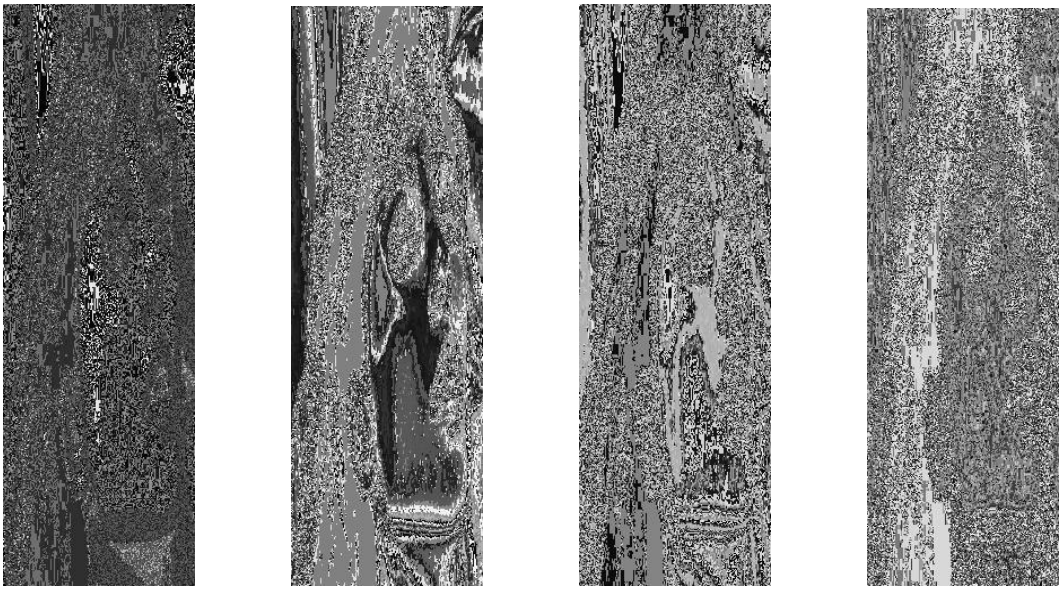


Fig 45 **Fig 46** **Fig 47** **Fig 48**

Fig 49: Reconstructed Image

Image name: child.jpg

Fig 50: Original Image

share1 share 2 share 3 share 4

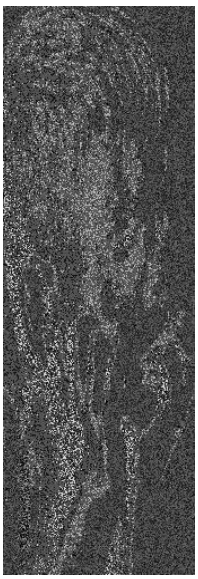


Fig 51

Fig 52

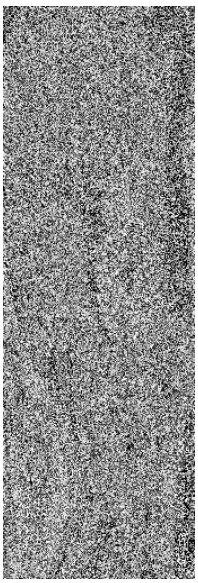


Fig 53

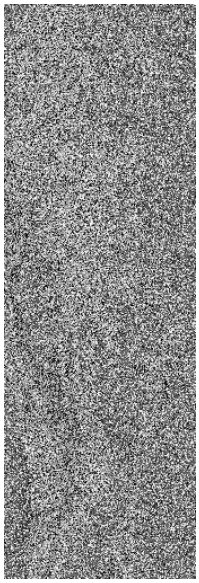


Fig 54

Reconstruction of original image using the shares

share1 share 2 share 3 share 4

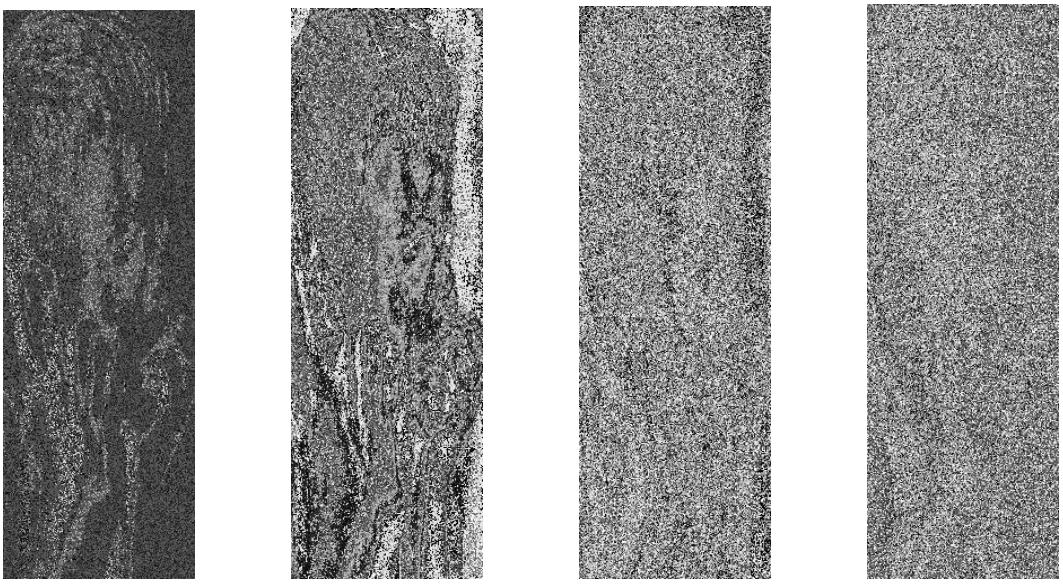


Fig 51 **Fig 52** **Fig 53** **Fig 54**

Fig 55: Reconstructed Image

Image name: fly.jpg

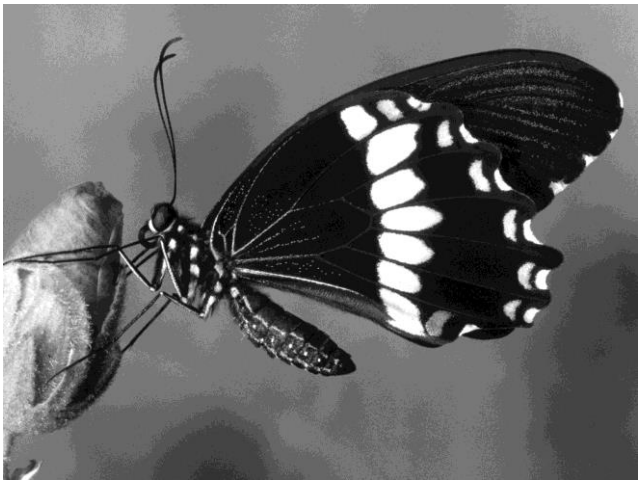


Fig 56: Original Image

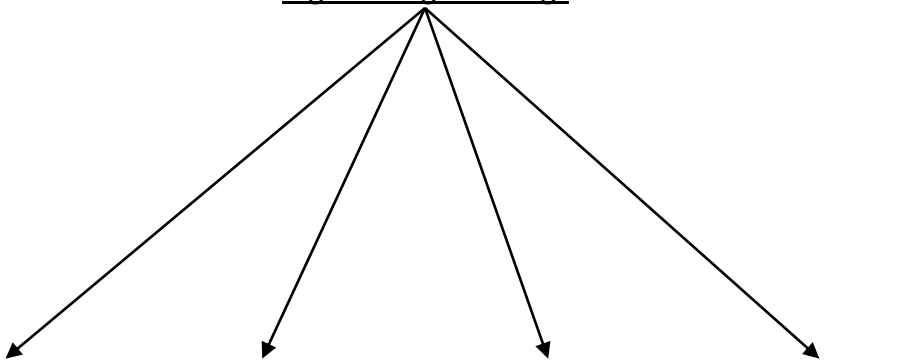


Fig 57

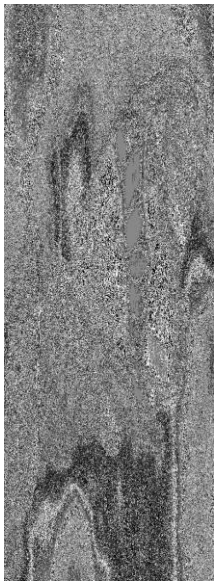


Fig 58

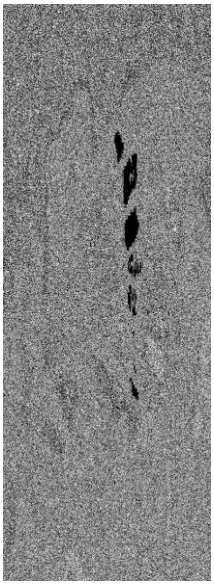


Fig 59

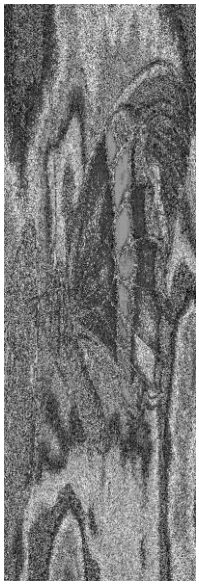


Fig 60

Reconstruction of original image using the shares

share1 share 2 share 3 share 4

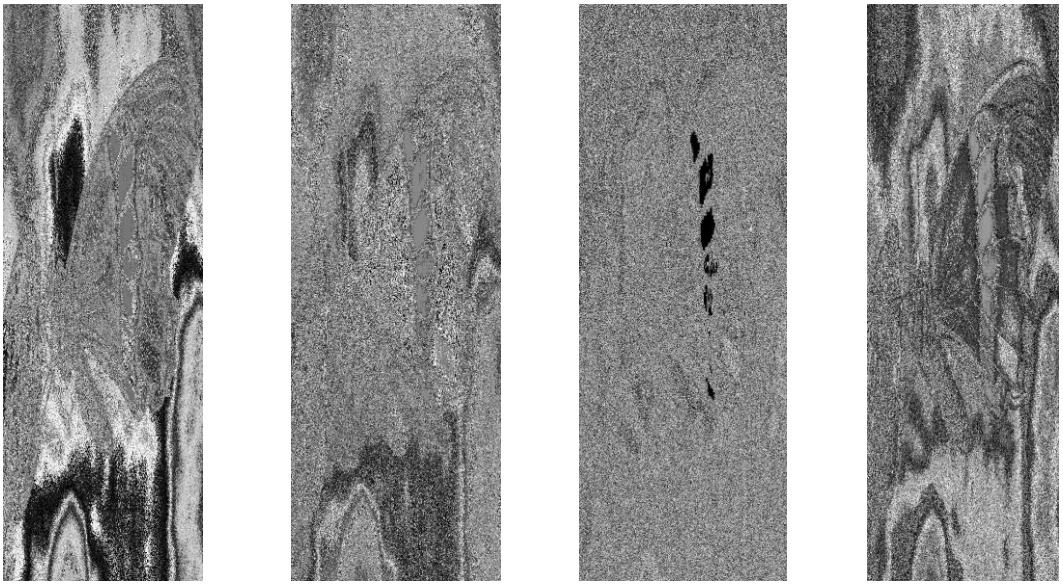


Fig 57 **Fig 58** **Fig 59** **Fig 60**

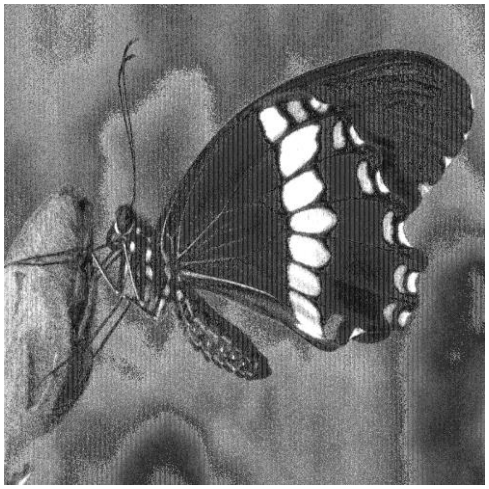
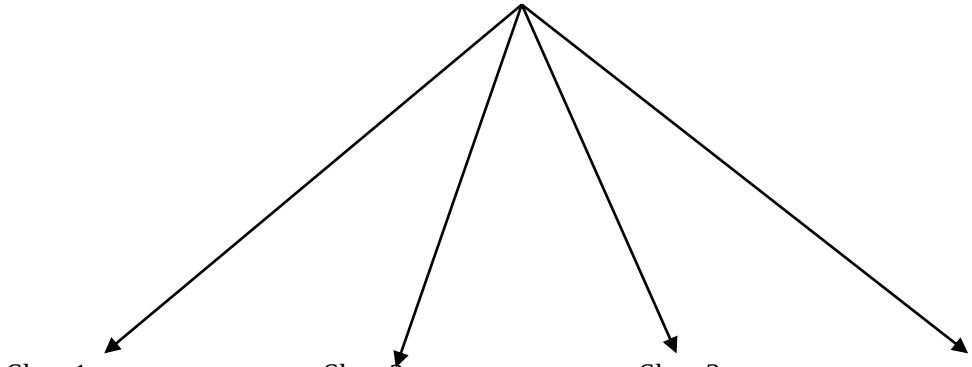


Fig 61 : Reconstructed Image

Image name: cameraman.jpg

Fig 62: Original Image



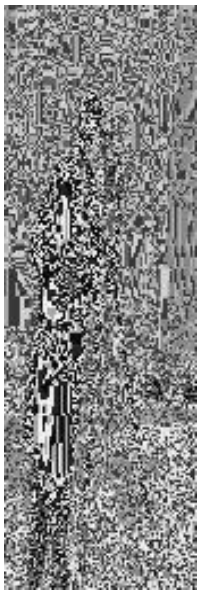


Fig 63

Fig 64

Fig 65

Fig 66

Reconstruction of original image using the shares

Share1 Share2 Share3 Share4

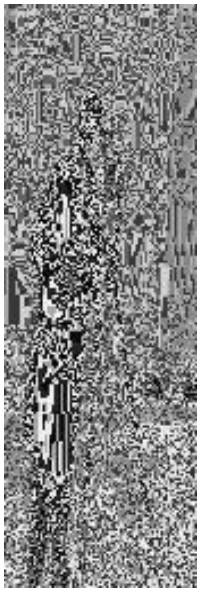
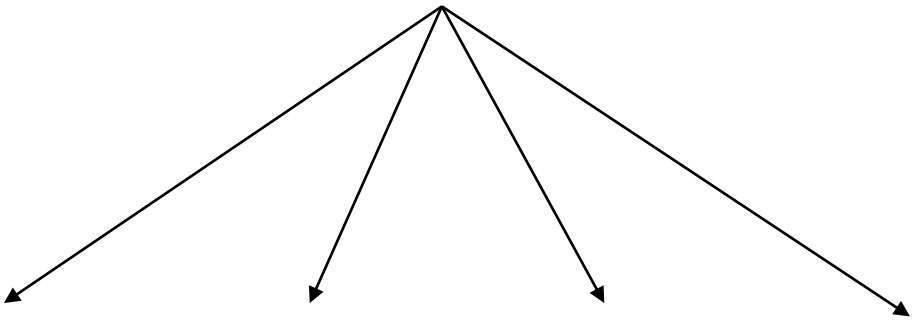


Fig 63 **Fig 64** **Fig 65** **Fig 66**

Fig 67: Reconstructed Image

Image name: duck.jpg

Fig 68: Original Image



Share1 Share2 Share3 Share4

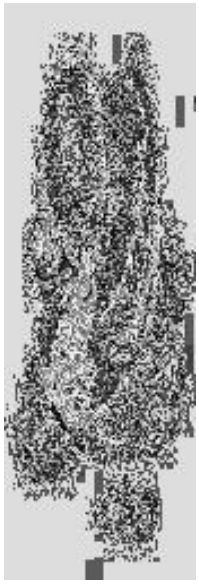


Fig 69

Fig 70

Fig 71

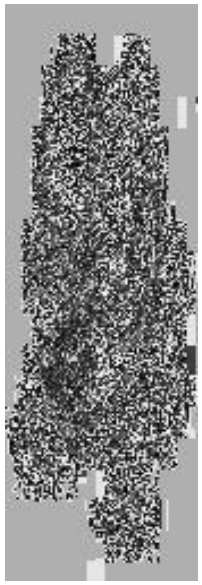


Fig 72

Reconstruction of original image using the shares

Share1 Share2 Share3 Share4

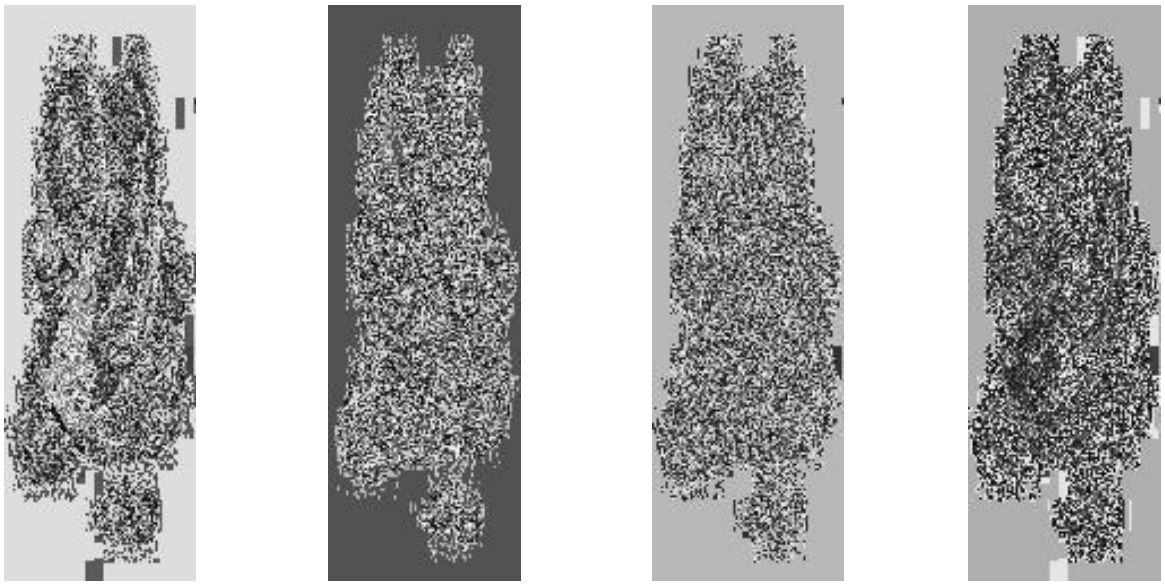


Fig 69 **Fig 70** **Fig 71** **Fig 72**

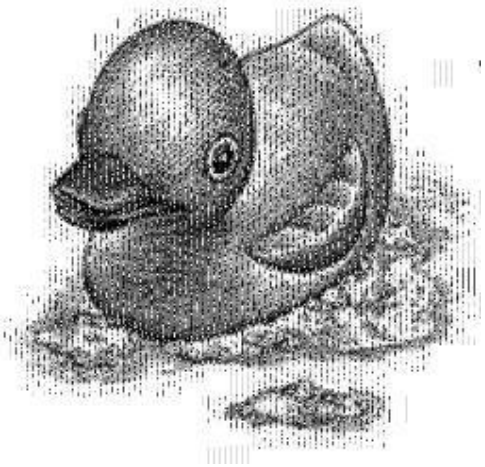


Fig 73: Reconstructed Image

Construction of Shares Using Three Pixel Method with Image name: airplane.jpg

Fig 74: Original Image

Share1 Share2 Share3 Share4

Fig 75

Fig 76

Fig 77

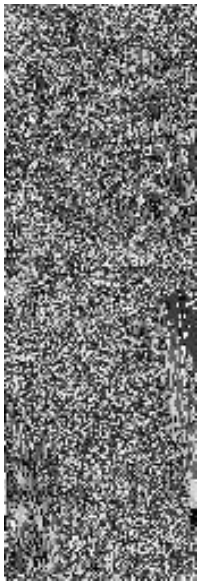


Fig 78

Reconstruction of original image using the shares

Share1 Share2 Share3 Share4

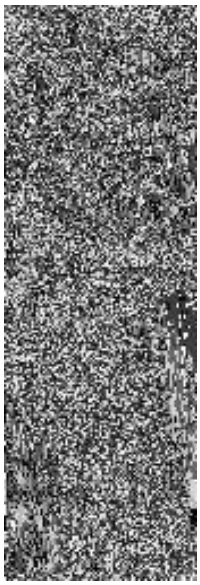


Fig 75 **Fig 76** **Fig 77** **Fig 78**

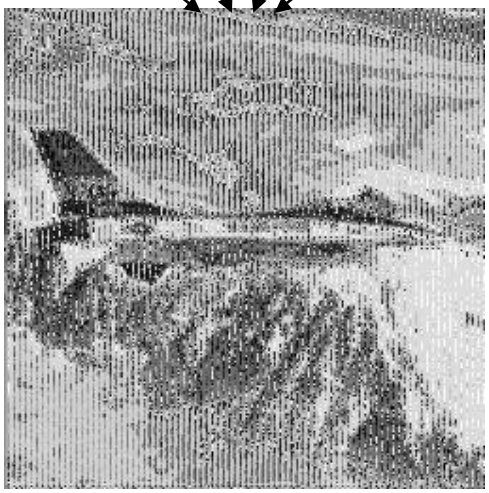


Fig 79: Reconstructed Image

PSNR Values for Share Construction Using Three Pixel Algorithm

Image Name:	**PSNR Values:**
Lena.jpg	**31.55dB**
Lady.jpg	**30.85dB**
Child.jpg	**31.17dB**
Fly.jpg	**31.25dB**
Cameraman.jpg	**31.43dB**
Duck.jpg	**30.57dB**
Airplane.jpg	**30.42dB**

Our PSNR values range between 30dB and 50dB.Hence our values are accurate.

CHAPTER 5

CONCLUSION:

We have given the theoretical background of various methods of attaining information security, the different Secret Sharing Schemes and studying the output derived from the reconstruction of an image using various sub pixel values that have been attained from the matrix (pixel) values of an image. The Secret Sharing method serves the purpose of making the information secure as the information is not decoded by an intruder and safely transmitted over the medium. Both the methods-One Pixel Method and Share Method have been used for this purpose and both of them show very good results in different aspects. Since there is a basic difference between both the approaches and both have their pros and cons so it is totally at the users wish and requirements to try and find out the suitable process for transmission depending on its priority. The evolution of the various outputs from the various sub pixel values is accounted in the above chapters.

The proposed method does not need complicated computation and that when only the required number of secret images is gathered can the secret image be reconstructed without any loss. We were successfully been able to reconstruct the image from the algorithms used to generate shares. It has given in depth the information that anyone cannot obtain any information from the stego media but only the person who owns the right key can only obtain the secret information correctly. We have included a few examples to improve the readability of the thesis and have tried to maintain the rigor of the treatment of the subject by first trying it with the Lagrange's Interpolation Formulae. When we found the output undesirable and less effective, we tried the construction and reconstruction of an image using the secret sharing scheme.

The One Pixel Method generates exceptionally good reconstructed image but the shortcoming is that the shares generated are not as concealing in nature as was the need of the hour. Since there are only One Pixels that are being generated from each pixel through two randomized matrix so the scrambled image i.e. the obtained shares are not very much impressive and the probability of guessing or reconstructing the image from individual shares is slightly higher as compared to the Three Pixel Method. The effective reconstruction is due to the fact that in this method, values are selected from [4x4] random matrix where the chances of obtaining redundant data is minimal so the noise in this case is less and we obtain almost the same image. Even though the image will not be completely decoded but the person concerned might get some idea regarding the message which might be used to adverse effects.

The Three Pixel Method is more productive, since security and integrity of the message is our prime criteria, and secure than the One Pixel Method. Since Three Pixels are generated from two pixels

using four randomized matrix so obtained shares are camouflaged (masked) in a very effective manner. The probability of reconstruction of the message from individual shares is very less so this method ensures satisfactory results in the field of security. However the reconstructed image obtained from the Three Pixels is slightly disoriented as compared to the One Pixel Method. The disorientation of the image is mainly because in this case we use [16x16] random matrix for the purpose of generation of the scrambled image i.e. the shares due to which the chances of getting redundant data is more. During reconstruction the same value might be present at different places which give us somewhat anomalous results in certain cases. In this case the noise is higher in the reconstructed image but it is acceptable since the obtained reconstructed image from the Three Pixels is reasonably good and our aim is fulfilled.

Both of these methods show satisfactory results in different fields of necessities and maintain optimum security and integrity level. There is always scope for improvement in everything that has been achieved so far. In spite of all the utilities this concept can still be worked upon in future to increase its effectiveness. The security and integrity issue can be taken care of by increasing the number of pixels used for the purpose of generating the scrambled image i.e. the shares as a result of which for every four values of pixels in the image we will be generating a single value in the share and similarly we can increase the number of shares by keeping the value of pixels unchanged. To enhance the security the shares generated can be masked by a cover media so that even if a person gets the cover image he/she won't be able to view the shares. These cover images would appear mere images to others and our shares will be secure. However, the intended recipient will retrieve the shares from these images and use the shares to reconstruct the original image.

The limitations and disadvantages of the various forms of secret sharing schemes are also brought out. We have also proved that the representation on increasing the number of sub pixel values each time we try to reconstruct an image, more security is attained. Being a new system, there is much scope for further development in this area. It has thus been introduced through the outputs of our project that Secret sharing has the potential of providing effective message security to its clients but with the limitation that when the messages are embedded into the cover media, how to preserve perceivable distortion is the main consideration. With the introduction of noise in our image, decryption shows poor results, thus leading to the conclusion that increase in the number of keys (sub pixels) generates shared images which is not understandable thus giving effective or satisfactory outputs.

We have obtained PSNR value ranging between 30 and 50 which indicates that our shares generate better reconstructed images compared to other secret sharing schemes.

CHAPTER 6

REFERENCES:

[1] Berry Schoenmakers, Department of Mathematics and Computing Science, Eindhoven University of Technology, The Netherlands. **A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting.** In Advances in Cryptology—CRYPTO '99, Vol. 1666 of Lecture Notes in Computer Science, Springer-Verlag, 1999. pp. 148-164.

[2] Giorgio Zanin, Dipartimento di Informatica, Universit `a degli Studi di, Roma "La Sapienza". **Secret Sharing Schemes and their Applications.** S.M.A.R.T. periodic meetings

[3] Helger Lipmaa, Helsinki University of Technology. Lecture 9: **Secret Sharing, Threshold Cryptography, MPC**. T-79.159 Cryptography and Data Security, 24.03.2004.

[4] Pablo Azar†,Harvard University '09 Cambridge, MA 02138. FEATURE 9: APPLIED MATHEMATICS CORNER. **Secret Sharing and Applications.**

[5] Ventzislav Nikov.Eindhoven: Technische Universiteit Eindhoven, 2005. CIP-DATA LIBRARY TECHNISCHE UNIVERSITEIT EINDHOVEN Nikov, Ventzislav S. **Verifiable Secret Sharing and Applications** / by Proefschrift. – ISBN 90-386-0574-9 NUR 918.
Subject headings: **cryptology / coding theory**
2000 Mathematics Subject Classification: 94A60, 94A62, 94B20, 11T71, 11Y16.

[6] Lecturer: Atri Rudra Scribe: Kanke Gao. Error Correcting Codes: Combinatorics, Algorithms and Applications (Fall 2007).Lecture 20: **Application: Secret Sharing** October 12, 2007.

[7] Lin Dong, Min Ku.Department of computer science abd technology.Tsinghua university. Beijing, China. **Novel (n, n) secret image sharing scheme based on addition**.2010 Sixth International Conference On Intelligent Information Hiding and Multimedia Signal Processing.

[8] Daoshan Wang, Lei Zhang, Ning Ma, Xiaobo, Department of computer Science and Technology,Tsinghua University,Beijing 100084,China. Department Of Computing Science, University Of Alberta, Edmonton. Alta.Canada. **Two Secret sharing schemes based on Boolean operations.**

[9]Hao-Kuan Tso, Der-Chyuan Lou, Dah-Lih Jeng, and Chao-Lung Chao Department of Electronic Engineering, Army Academy R.O.C., Chungli, Taiwan.Department of Electrical and Electronic Engineering, Chung Cheng Institute Of Technology, Taiwan. Department of Computer Science, Chung Cheng Institute of Technology, Taiwan**. Secret sharing Method for Gray-Level Images**. 2009 Fifth International Conference On Intelligent Information Hiding and Multimedia Signal Processing.