

**ANALYSIS AND DESIGN OF SECURE VISUAL
SECRET SHARING SCHEMES WITH ENHANCED
CONTRAST**

Thesis

Submitted in partial fulfilment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

by

NIKHIL CHANDRAKANT MHALA



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA

SURATHKAL, MANGALORE - 575 025

August, 2021

DECLARATION

by the Ph.D. Research Scholar

I hereby declare that the Research Thesis entitled **ANALYSIS AND DESIGN OF SECURE VISUAL SECRET SHARING SCHEMES WITH ENHANCED CONTRAST** which is being submitted to the **National Institute of Technology Karnataka, Surathkal** in partial fulfilment of the requirements for the award of the Degree of **Doctor of Philosophy** in Department of Computer Science and Engineering is a bonafide report of the research work carried out by me. The material contained in this Research Thesis has not been submitted to any University or Institution for the award of any degree.



Nikhil Chandrakant Mhala

Register No. 165035 CS16F03

Department of Computer Science and Engineering

Place: NITK, Surathkal.

Date: August 11, 2021

CERTIFICATE

This is to certify that the Research Thesis entitled **ANALYSIS AND DESIGN OF SECURE VISUAL SECRET SHARING SCHEMES WITH ENHANCED CONTRAST** submitted by **NIKHIL CHANDRAKANT MHALA** (Register Number: 165035 CS16F03) as the record of the research work carried out by him, is accepted as the Research Thesis submission in partial fulfilment of the requirements for the award of degree of **Doctor of Philosophy**.

Dr. Alwyn Roshan Pais

Research Guide

(Signature with Date and Seal)

Chairman - DRPC

(Signature with Date and Seal)

ACKNOWLEDGEMENTS

Foremost, I would like to express my sincere gratitude to my Supervisor Dr. Alwyn R Pais, Associate Professor in Department of CSE for his continuous encouragement, patience, motivation, enthusiasm, and immense knowledge. His guidance and insightful comments helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for this thesis.

My sincere thanks go to research progress committee members Dr. Jeny Rajan, Assistant Professor in Department of CSE and Dr. A. V. Narasimhadhan, Assistant Professor in Department of E&C, for giving their valuable suggestions, inspiration and moral support while evaluating our work time to time. I am also grateful to all of-office staff members of Computer Science & Engineering Department for their generous support throughout this work.

Thank our ISEA lab members- Srinivas, Alok, Apurva, Ajnas, Somesh, Raviraja Holla, Zubair, and K Sivakumar for their suggestions and support during this journey. Special thanks to my roommate Pramod and my classmate Amith for supporting me throughout the PhD. journey. A special thanks go to the married researchers, Mr. & Mrs. Sachin Patil, Dr. Vishnu Yeralagadda, and Vishal Rathod for their delicious homemade food. I extend special thanks to my motivators, correctors, playing partners, and trekkers Vishal Rathod, Pravin Ramteke, Bheemappa Halawar, Pradyoth Hegde, and Raghavan.

Last but not least, I am incredibly grateful to my family members- father, sisters, brothers, brothers-in-law, for their unconditional love, constant support, motivation, and encouragement in my life.

Nikhil Chandrakant Mhala

ABSTRACT

The Visual Secret Sharing (VSS) scheme is a cryptography technique, which divides the secret image into multiple shares. These shares are then transmitted over a network to respective participants. To recover the secret image, all participants must have to stack their shares together at the receiver end. [Naor and Shamir \(1994a\)](#) first proposed basic VSS scheme for binary images using threshold scheme. The scheme generated shares with increased sizes, hence it suffered from the problem of expanded share. To overcome the problem of expanded shares, Block-based Progressive Visual Secret Sharing (BPVSS) scheme was proposed by [Hou et al. \(2013a\)](#). BPVSS is an effective scheme suitable for both gray-scale and color images. Although BPVSS scheme recovered secret image with better quality, it still suffers from the problems like 1) The restored image obtained by joining all the shares together always results in a binary image. 2) The maximum contrast achievable by BPVSS is 50%. This thesis presents various mechanisms to improve reconstruction quality and the contrast of a secret image transmitted using BPVSS.

First technique proposed by thesis is Randomised Visual Secret Sharing (RVSS) [\(Mhala et al. 2018\)](#). The RVSS is an encryption technique that utilises block-based progressive visual secret sharing and Discrete Cosine Transform (DCT) based reversible data embedding technique to recover a secret image. The recovery method is based on progressive visual secret sharing, which recovers the secret image block by block. The existing block based schemes achieve the highest contrast level of 50% for noise-like and meaningful shares. The presented scheme achieves a contrast level of 70-90% for noise-like and 70-80% for meaningful shares. The enhancement of contrast is achieved by embedding additional information in the shares using DCT-based reversible data embedding technique. Experimental results showed that the proposed scheme restores the secret image with better visual quality in terms of human visual system based parameters

Although RVSS scheme recovers secret images with a better contrast; the scheme still suffers from the problems of blocking artifacts. To further improve the reconstruction quality of the RVSS, this thesis presents a novel Super-resolution based Visual Secret Sharing (SRVSS) technique. The SRVSS scheme used super-resolution concept along with data hiding technique to improve the contrast of the secret images. The experimental results showed that the SRVSS scheme achieves the contrast of 70-80% for meaningful shares and 99% for noise-like shares. Also, scheme recovers the secret image free from blocking artifacts.

Nowadays, medical information is being shared over the communication networks due to ease of technology. The patient's medical information has to be securely communicated over a network for Computer Aided Diagnosis (CAD). Most of the communication networks are prone to attacks from an intruder thus compromising the security of patients data. Therefore, there is a need to transmit medical images securely over a network. Visual secret sharing scheme can be used to transmit the medical images over a network securely. This thesis has applied the super-resolution based VSS scheme on the medical images to transmit them over a network. The experimental results showed that, scheme recovers medical images with better contrast. The experimental results showed that the presented system is able to reconstruct the secret image with the contrast of almost 85-90% and similarity of almost 77%. Additionally, the performance of the presented system is evaluated using the existing CAD systems. The reconstructed images using the presented super-resolution based VSS scheme achieves the similar classification accuracy as that of existing CAD system.

Nowadays, underwater images are being used to identify various important resources like objects, minerals, and valuable metals. Due to the wide availability of the Internet, the underwater images can be transmitted over a network. As underwater images contain important information, there is a need to transmit them securely over a network. Visual secret sharing (VSS) scheme is a cryptographic technique, which is used to transmit visual information over insecure networks. Randomized VSS (RVSS) scheme recovers Secret Image (SI) with a Self-Similarity index (SSIM) of 60-80%. But, RVSS is suitable for general images, whereas underwater images are more com-

plex than general images. The work presented in the thesis to share underwater images over a network uses a super-resolution based VSS scheme. Additionally, it has removed blocking artifacts from the reconstructed secret image using Convolution Neural Network (CNN)-based architecture. The presented CNN-based architecture uses a residue image as a cue to improve the visual quality of the SI. The experimental results show that the presented VSS scheme can reconstruct SI with almost 86-99% SSIM. Hence can be used to transmit complex images over a insecure channels.

Keywords: Visual Cryptography, Visual Secret Sharing, Discrete Cosine Transform, Super-resolution.

CONTENTS

List of Figures	xiv
List of Tables	xvi
List of Abbreviations	xvii
1 Introduction	1
1.1 Introduction to Visual Cryptography	1
1.2 Basic VC Model	3
1.2.1 An example of Basic 2-out-of-2 VCS	5
1.3 Motivation	6
1.4 Thesis Contributions	8
1.5 Thesis Organization	9
2 Literature Review	11
2.1 Traditional Visual Secret Sharing Schemes	11
2.1.1 VSS for gray level images	15
2.1.2 VSS for color images	17
2.2 Progressive Visual Secret Sharing Schemes	18
2.3 Reversible Data Hiding Techniques	24
2.4 Super Resolution	25
2.4.1 Multiple Image Super Resolution	25
2.4.2 Single Image Super Resolution (SISR)	26
2.5 Problem Description	26
2.6 Problem Statement	27
2.7 Objectives	27
2.8 Summary	27

3	Randomized Visual Secret Sharing (RVSS) Scheme	29
3.1	Randomized Visual Secret Sharing (RVSS) Scheme	31
3.1.1	Generation of shares	32
3.1.2	Embedding of data into shares	37
3.1.3	Extraction of data and reconstruction of image	42
3.1.4	Embedding data back into image	45
3.2	Experimental results	45
3.2.1	Mean Square Error -HVS (MSE^{HVS})	46
3.2.2	Peak Signal-to-Noise Ratio (PSNR)	47
3.2.3	Normalized Cross Correlation (NCC)	48
3.2.4	Normalized Absolute Error (NAE)	49
3.3	Summary	52
4	Contrast enhancement of Random Visual Secret Sharing scheme	53
4.1	A super-resolution based Visual Secret Sharing (SRVSS) scheme	54
4.1.1	Share generation using BPVSS	56
4.1.1.1	Preliminaries for generating shares	56
4.1.1.2	Share Generation Algorithm	59
4.1.2	Embedding secret image information into shares	61
4.1.2.1	Pixel embedding procedure	63
4.1.3	Extraction of embedded data and low resolution image formation	64
4.1.3.1	Extraction of embedded data from shares	65
4.1.3.2	The low resolution image formation	66
4.1.4	Contrast enhancement of recovered image using Super-resolution	67
4.2	Experimental results	71
4.2.1	Mean square error (MSE^{HVS})	73
4.2.2	Peak-signal to noise ratio (PSNR)	75
4.2.3	Normalized Cross-correlation (NCC)	75
4.2.4	Normalized absolute error (NAE)	78
4.2.5	Structural Similarity Index (SSIM)	78
4.3	Summary	83

5 Applications of the Visual Cryptography	85
5.1 The Secure Visual Secret Sharing (VSS) scheme for Medical Images . . .	86
5.2 VSS scheme for Medical images	87
5.2.1 Generation of shares using BPVSS	88
5.2.2 Embedding low-resolution image information into shares	89
5.2.3 Extraction of embedded data from shares	89
5.2.4 Recovery of the secret image using XOR operation	90
5.2.5 Low resolution image formation	91
5.2.6 Contrast enhancement of the recovered image using Super Res-	
olution	91
5.3 Experimentation Results	93
5.3.1 The visual quality of the reconstructed image	93
5.3.2 The performance of the proposed system for Computer Aided	
Diagnosis (CAD)	94
5.4 The Secure Visual Secret Sharing Scheme for Underwater images . . .	97
5.5 The Super-resolution based Visual Secret Sharing (SRVSS) Scheme . . .	99
5.5.1 Reconstruction of the secret underwater image using SR	102
5.6 Image Enhancement using Convolution Neural Network	103
5.6.1 Initialize the artifact-free image using ARCNN	103
5.6.2 Generate the residual image using deep CNN model	105
5.6.3 Generate the final output image	106
5.7 Experimental Results	106
5.7.1 Image quality Evaluation metrics	106
5.7.1.1 Self-similarity index (SSIM)	107
5.7.1.2 Mean Square Error (MSE)	107
5.7.1.3 Normalized Cross Correlation (NCC)	107
5.7.1.4 Normalized Absolute Error (NAE)	108
5.7.2 Experiment 1: Performance evaluation of SR based VSS scheme	108
5.7.3 Experiment 2: Performance of the proposed system after apply-	
ing CNN-based image enhancement architecture	111

5.8 Summary	115
6 Conclusions and Future Scope	117
Bibliography	120
Research Outcomes	132

LIST OF FIGURES

1.1 Basic model of traditional cryptography	2
1.2 Basic model of visual cryptography	3
1.3 Shares generated for white/black pixel using basis matrices given in Equation 1.4. First column indicates white/black pixel, column two and third indicates visual representation of share 1 and share 2, and last column indicates OR of column two and three	6
1.4 Sample output of the 2-out-of-2 VCS (a) Original secret image, (b) generated Share 1, (c) generated shares 2, and (d) output image after stacking share 1 and share 2 together using simple 'OR' operation	7
2.1 Basis matrices for 2 out of 2 scheme (m=4). First column indicates white/black pixel, column two and third indicates visual representation of share 1 and share 2, and last column indicates OR of column two and three	12
2.2 A sample example for 2 out of 2 scheme (m=4). (a) Original secret image, (b) generated Share 1, (c) generated shares 2, and (d) output image after stacking share 1 and share 2 together using simple 'OR' operation	13
2.3 Shares generated using EVCS (a) secret image, (b-d) shares generated with meaningful cover image, (e) output after stacking share 1 and 2 together, (f) output after stacking share 2 and 3 together and (g) output of EVCS after stacking share1, 2 and 3 together	14

2.4	Size invariant shares generation using Ito et al. (1999)'s scheme. (a) Original secret image, (b) recovered secret image using (2,3) VSS, and (c) recovered secret image using all (3,3) shares	15
2.5	An example of Halftone technique. (a) the original image, and (b) Halftone image generated for original image	15
2.6	Overview of the gray-scale VSS system based on halftone technology .	16
2.7	General color model used for VSS. (a) Additive color model, (b) Subtractive color model	17
2.8	Color image visual cryptography (Hou 2003) example using CMY color model	18
2.9	PVSS: Recovering entire image gradually. (a) share 1 (b) stacked share 1 and share 2 (c) stacked shares 1- 3, (d) Stacked shares 1-4, (e) stacked shares 1-5, and (f) output of all the shares stacked together	19
2.10	PVSS: Recovering secret image block by block . (a) share 1 (b) stacked share 1 and share 2 (c) stacked shares 1- 3, (d) Stacked shares 1-4, (e) stacked shares 1-5, and (f) output of all the shares stacked together	20
3.1	Overview of the RVSS (Mhala et al. 2018) system. 1) Generation of shares S_1, S_2, \dots, S_n , 2) Embedding of data into shares S_1, S_2, \dots, S_n , 3) Extraction and reconstruction of image, 4) embedding data back into shares	31
3.2	Sample shares generated using BPVSS scheme for a man.tiff image. (a) The original image man.tiff of size 1024 x 1024, (b) The four shares generated for the original image S_1, S_2, S_3 and S_4	32
3.3	Meaningful cover generated for (a) Original image, (b) Shares generated S_1, S_2, S_3 , and S_4 having another image as cover	33
3.4	Block patterns used by proposed system. (a) The pattern 1 having 4 blocks, (b) The pattern 2 having 4 blocks.	34
3.5	Nine sets defined for data embedding	39
3.6	The sample original color images used for the experiment as (a) Girl, (b) Couple, (c) House, and (d) Tree	50

3.7	Output of BPVSS (Hou et al. [2013a]) scheme for color images. (a) Girl, (b) Couple, (c) House, and (d) Tree	50
3.8	Output of RVSS (Mhala et al. [2018]) scheme for color images. (a) Girl, (b) Couple, (c) House, and (d) Tree	51
3.9	Gray-scale images used for experiment as (a) Airplane, (b) Clock, (c) Couple, (d) Man	51
3.10	Output of BPVSS (Hou et al. [2013a]) scheme for gray-scale images a) Airplane, (b) Clock, (c) Couple, (d) Man	51
3.11	Output of RVSS (Mhala et al. [2018]) scheme for gray-scale images a) Airplane, (b) Clock, (c) Couple, (d) Man	51
4.1	The Flowchart of the SRVSS system	55
4.2	The sample input images used : (a) the secret image (lenna.tiff) (SI) (b) Halftone image generated from secret image (SI_{halftone})	57
4.3	The shares generated for four participants. (a) Share of participant 1 (SI₁) (b) Share of participant 2 (SI₂) (c) Share of participant 3 (SI₃) and (d) Share of participant 4 (SI₄)	57
4.4	(a) The embedded secret image information into the shares (b) The re- stored image by applying XOR operation on shares (SI_{xor})	63
4.5	(a) The embedded secret image information into the shares (b) The re- stored image by applying XOR operation on shares (SI_{xor})	64
4.6	(a) Recovered secret image information having size of 128×128 (b) The image used as initial guess to solve SR problem (c) The final restored image having size 512×512 in the gray-scale format	66

4.7	Overview of the low resolution image formation: (a) The extracted hidden image from shares (128×128) (b) The restored shares for four participants ($\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3, \mathbf{S}_4$) (512×512) (c) The recovered secret image (\mathbf{SI}_{xor}) by stacking shares $\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3, \mathbf{S}_4$ using XOR operation (512×512) (d) The image obtained after applying Gaussian blur on the \mathbf{SI}_{xor} image (512×512) (e) The first low resolution observation ($\mathbf{L1}$) (128×128) (f) The second extracted low resolution observation ($\mathbf{L2}$) (128×128) (g) The third low resolution image ($\mathbf{L3}$) (128×128).	68
4.8	The sample shares generated for secret image: (a) The secret Image (b) The four meaningful shares generated for respective participants	72
4.9	The sample test (gray-scale) images used by proposed system (a) Airplane, (b) Clock, (c) Couple, (d) Man	73
4.10	The sample test (Color) images used by proposed system (a) Girl, (b) Couple, (c) House, and (d) Tree	73
4.11	The sample outputs of BPVSS scheme (Color images) (a) Girl (b) Couple, (c) House, and (d) Tree	80
4.12	The sample outputs of RVSS scheme (color images) (a) Girl (b) Couple, (c) House, and (d) Tree	80
4.13	The sample outputs of BPVSS scheme for gray-scale images (a) Airplane, (b) Clock, (c) Couple, and (d) Man	80
4.14	The sample outputs of RVSS scheme for gray-scale images (a) Airplane, (b) Clock, (c) Couple, and (d) Man	82
4.15	The sample output of the SRVSS scheme for color images (a) Girl, (b) couple, (c) House, and (d) tree	82
4.16	The sample output of the SRVSS scheme for gray-scale images (a) airplane, (b) clock, (c) couple, and (d) man	83
5.1	The overview of the proposed system	87
5.2	Sample test images used for experimentation and the reconstructed images using RVSS (Mhala et al. [2018]) and proposed scheme	94

5.3	The Overview of the Super-resolution based VSS scheme for transmission of underwater images	100
5.4	Four shares generated by the proposed technique for the input image (for n = 4 participants) (a) Original input image, (b-d) shares generated for 4 participants	101
5.5	Low-resolution image formation (a) The L1 observation: extracted from the shares. (b) The L2 observation: formed by stacking the restored shares together, and (c) The L3 observation: obtained by applying Gaussian blur on L2	101
5.6	The proposed CNN-based image enhancement architecture for SRVSS	102
5.7	A sample output for reconstruction of secret Chlorophyll (Font view) underwater image. (a) The original underwater image, (b) Reconstructed underwater image using the RVSS scheme, (c) reconstructed underwater image using the SRVSS scheme, (d) the underwater image after removal of artifacts using ARCNN, and (e) final reconstructed underwater image using CNN-based VSS scheme. (The original image too large for display, hence only part of an image is shown for better visualization)	103
5.8	Overview of the ARCNN architecture for removal of artifacts	104
5.9	Reconstruction of secret Chlorophyll (Side view) underwater image. (a) The original underwater image, (b) Reconstructed underwater image using the RVSS scheme, (c) reconstructed underwater image using the SRVSS scheme, (d) the underwater image after removal of artifacts using ARCNN, and (e) final reconstructed underwater image using CNN-based VSS scheme. (The original image too large for display, hence the only part of an image is shown for better visualization)	110

5.10 Reconstruction of secret Deep underwater image. (a) The original un-	
derwater image, (b) Reconstructed underwater image using the RVSS	
scheme, (c) reconstructed underwater image using the SRVSS scheme,	
(d) the underwater image after removal of artifacts using ARCNN, and	
(e) final reconstructed underwater image using CNN-based VSS scheme.	
(The original image too large for display, hence the only part of an im-	
age is shown for better visualization)	110
5.11 Reconstruction of the secret underwater image with added milk turbid-	
ity. (a) The original underwater image, (b) Reconstructed underwa-	
ter image using the RVSS scheme, (c) reconstructed underwater image	
using the SRVSS scheme, (d) the underwater image after removal of	
artifacts using ARCNN, and (e) final reconstructed underwater image	
using CNN-based VSS scheme. (The original image too large for dis-	
play, hence the only part of an image is shown for better visualization)	
	111

LIST OF TABLES

2.1 Overview of visual secret sharing schemes	21
2.2 Pros and Cons of Visual Secret Sharing (VSS) schemes	23
3.1 Generated basis matrices for $n = 4$	36
3.2 The standard quantization table	40
3.3 Size of each chosen sets for embedding. k is the set number and $K(k)$ indicates the size of the respective set	41
3.4 Mean square error-HVS value for various test images	47
3.5 Peak signal-to-noise ratio (PSNR) value for various test images (in dB).	48
3.6 Normalized Cross Correlation (NCC) value for various test images	49
3.7 Normalized Absolute Error (NAE) value for various test images	50
4.1 Generated basis matrices for $n = 4$	58
4.2 Mean square error-HVS value for various test images	74
4.3 Peak signal-to-noise ratio (PSNR) value for various test images (in dB).	76
4.4 Normalized Cross Correlation (NCC) value for various test images	77
4.5 Normalized Absolute Error (NAE) value for various test images	79
4.6 Structural Similarity Index (SSIM) value for various test images	81
5.1 The average values of HVS parameters for all medical images	93
5.2 BOF approach with SIFT features (300 and 500 clusters)	96
5.3 BOF approach with SIFT features (1000 clusters)	96
5.4 BOF approach with DCT features (300 and 500 clusters)	96
5.5 BOF approach with DCT features (1000 clusters)	97
5.6 The average values of HVS parameters for Chlorophyll (front view) images (The sample image is shown in Figure 5.7)	108

5.7	The average values of HVS parameters for Chlorophyll (side view) images (The sample image is shown in Figure 5.9)	109
5.8	The average values of HVS parameters for Deep Blue images (The sample image is shown in Figure 5.10)	109
5.9	The average values of HVS parameters for images with milk turbidity (The sample image is shown in Figure 5.11)	109
5.10	The network summary used by proposed system	112
5.11	The details of each layer used in a deep CNN network to predict the residual image	114

LIST OF ABBREVIATIONS

<u>Abbreviations</u>	<u>Expansion</u>
BPVSS	Block-based Progressive Visual Secret Sharing
CAD	Computer Aided Diagnosis
CNN	Convolution Neural Network
DCT	Discrete Cosine Transformation
EVCS	Extended Visual Cryptography Scheme
GAS	General Access Structure
HR	High Resolution
HVS	Human Visual System
IDCT	Inverse Discrete Cosine Transform
JL-DCF	Joint Learning and Densely-cooperative Fusion
LR	Low-resolution
MISR	Multiple Image Super-resolution
MSE	Mean Square Error
NAE	Normalized Absolute Error
NCC	Normalized Cross Correlation
PSNR	Peak Signal to Noise Ratio
PVSS	Progressive Visual Secret Sharing
RVSS	Randomized Visual Secret Sharing
SI	Secret Image
SR	Super-resolution
SRVSS	Super-resolution based Visual Secret Sharing
SISR	Single Image Super-resolution
SSIM	Self-Similarity index
VC	Visual Cryptography
VCS	Visual Cryptography Scheme
VSS	Visual Secret Sharing

CHAPTER 1

INTRODUCTION

Nowadays usage of Internet is becoming popular among people, facilitating them to share information over the network. Also, use of digital media is growing parallelly with the technology to share information. As huge data is getting exchanged over the Internet, many intruders try to steal the information. Recently, many cases are arising of stealing or replicating information over the network without authorization. The use of algorithms, techniques has become a need of technology to protect the data and information.

Hackers or intruders always try to steal or replicate information from multiple nodes. Also, sometimes users do not have faith in each other regarding preserving sensitive information. In such cases, there is a need to provide a solution which allows users to share information securely over multiple channels. The secret sharing is the scheme which provides solution to the above problem. The concept of secret sharing is to divide information into multiple pieces, so that the pieces of qualified users can reveal the secret information. The secret sharing scheme restricts user to come together in order to recover information. The scheme ensures that individual user should not recover the secret information.

1.1 INTRODUCTION TO VISUAL CRYPTOGRAPHY

Cryptography is a technique that has been used to conceal the secret information from unauthorized users. It provides security to the secret message by encrypting it. The

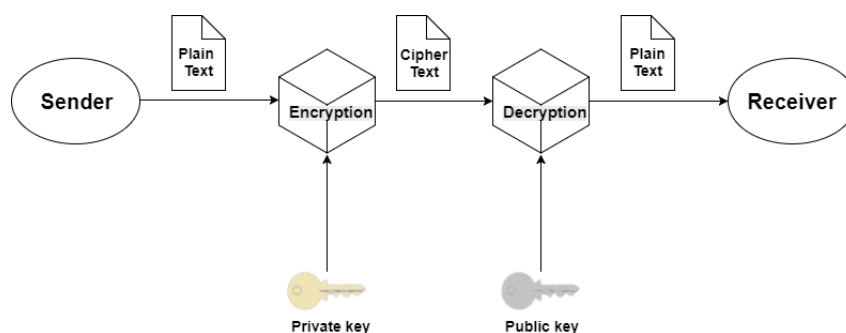


Figure 1.1: Basic model of traditional cryptography

encrypted information can be transmitted over the Internet without revealing a secret message. The basic steps involved in transmitting messages over the network are:-

- Encryption of the message using sender's secret key.
- Transmission of sender's public key and ciphertext over the network.
- Decryption of the message using sender's public key and receiver's private key.

Figure [1.1](#) gives an overview of traditional cryptography. The message which user want to transmit is known as plain text. Sender uses secret key to encrypt plain text and generates cipher text. Cipher text generated is unintelligible to outsiders. Decryption is the reverse operation of encryption. It gets back plain text from cipher text using public key shared by the sender. Cryptography is not the only means of providing information security, rather it is one of the technique among many. The traditional cryptography technique needs keys to be shared. Also, it involves complex algorithms and computation to encrypt and decrypt messages.

The visual cryptography was first introduced by [Naor and Shamir \(1994a\)](#). Visual Cryptography (VC) is a modern cryptography technique that protects visual information (text, image, etc.). The VC method was basically designed for binary images. The VC method provides a secure way to share images among n users. It generates n different noise-like shares using simple mathematical operations. Whenever users want to recover image they just need to stack their shares. Once all the users stack their shares together then secret information can be viewed by Human Visual System (HVS). The

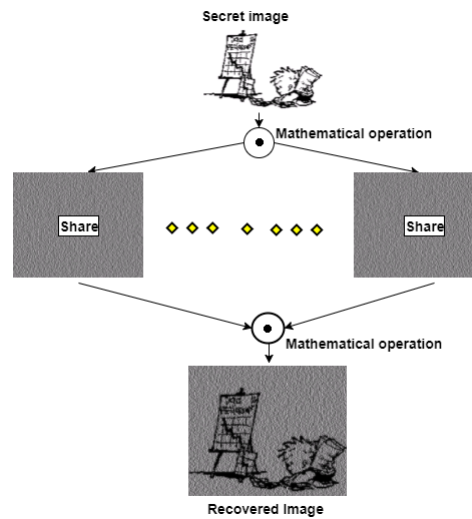


Figure 1.2: Basic model of visual cryptography

VC do not need any complex operations to decrypt the secret image, simple stacking operation can recover the image. Figure 1.2 shows the basic model of VC. Figure 1.2 shows that the secret image can be encrypted into n shares using mathematical operations. For decryption, it only needs a simple stacking operation to recover secret image. It is evident from Figure 1.2, that the recovered image can be perceived by Human Visual System (HVS). The advantages of visual cryptography are :-

- It is easy to implement.
- It uses simple mathematical operation to encrypt and decrypt visual information.
- It provides perfect secrecy to visual data making it more secure.
- It do not require any keys to be shared among each other.

1.2 BASIC VC MODEL

Naor and Shamir (1994a) first proposed basic Visual Secret Sharing (VSS) scheme for binary images. The scheme proposed by Naor and Shamir (1994a) requires at-least k shares out of n to be stacked together to recover secret image. It is also referred as k -out-of- n Visual Cryptography Scheme (VCS). Visual cryptography for two participants

can be formulated using two boolean matrices namely $S0$ and $S1$ having sizes of $n \times m$ known as basis matrices. Here m is defined as the pixel expansion for the original image pixel and n is number of participants. Additionally α represents relative difference and β represents contrast of an image. The basis matrices are being used for encrypting original image pixel. If original image pixel is white, then $S0$ is used to generate share. Similarly, if it is a black pixel then $S1$ is used to generate share. In order to construct the basis matrices, they should satisfy Definition 1 (Naor and Shamir 1994a) in order to construct secure and efficient k -out-of- n VCS.

Definition 1 :- The k -out-of- n VCS is said to be valid if and only if they hold following conditions with parameters $1 \leq d \leq m$ and $\alpha > 0$:

1. For white pixel from original image, the chosen $S0$ matrix should satisfy $H_w(V) \leq d - \alpha \cdot m$, where V is "or" of any k of the n rows.
2. For black pixel from image the chosen $S1$ matrix should satisfy $H_w(V) \geq d$, where V is "or" of any k of the n rows.
3. For any set $\{P_1, P_2, \dots, P_r\} \subset \{1, 2, \dots, n\}$ with $r \leq k$ the matrix $r \times m$ should have the total number of rows equal to the permutation of column for basis matrices $S0$ and $S1$.

Where $H_w(V)$ is the hamming weight (i.e. number of ones in the rows) of the V -vector, m is the pixel expansion and α is the *relative difference* of the image. The first two conditions ensure minimum contrast in the recovered image. The third condition ensures security in the shares formation. The above three condition makes VCS as secure and simple. VCS recovers image by stacking them together. VCS do not require any complex computation to recover image as compared to traditional cryptographic algorithm. The relative difference (α) and contrast (β) can be computed using formula given in 1.1 and 1.2 respectively.

Relative Difference (α) :- It is defined as the ratio of difference between the hamming weight of basis matrices $S0$ and $S1$ to the pixel expansion m .

$$\alpha = \frac{H_w(S1) - H_w(S0)}{m} \quad (1.1)$$

Contrast (β) :- It is the degree of measure for image visual quality by Human Visual System (HVS). It is defined as the product of relative difference α and pixel expansion m .

$$\beta = \alpha.m, \quad \beta \geq 1 \quad (1.2)$$

To recover visually identifiable image by Human Visual System, contrast (i.e. for VCS application) should be greater than one. With the help of Definition 1 basic 2-out-of-2 VCS to share secret image among two users has been explained below.

1.2.1 An example of Basic 2-out-of-2 VCS

The 2-out-of-2 VCS generates two noise-like shares. The shares themselves do not possess any information about the secret image. After stacking the two shares together, secret image gets revealed. In order to generate two noise-like shares one needs to form the basis matrices that satisfies Definition 1. For basic 2-out-of-2 VCS scheme, define the basis matrix of size 2×2 having pixel expansion ratio as 2. Pixel expansion parameter m indicates length of replacement pixel in the generated share. For example, to mask white/black pixel of original image, replace each pixel with two pixels in share resulting in expansion of shares. Consider the basis matrix S_0 and S_1 as shown in Equation 1.3 used for generating shares.

$$S_0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \quad S_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (1.3)$$

In order to generate shares, select the respective row elements from basis matrix S_0 and S_1 and assign it to shares (i.e. row 1 for share 1 and row 2 for share 2). To maintain the security, randomness is used to generate basis matrices. The possible combinations of valid basis matrices can be formulated by permuting the columns of S_0 for white pixel and S_1 for black pixel. The possible combination for white and black pixel are shown in Equation 1.4.

$$C^0 = \left(\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right) \quad C^1 = \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right) \quad (1.4)$$

To generate shares, user randomly selects one of the basis matrix from C^0 for white pixel and C^1 for black pixel respectively. Since selection of shares is random intruder can not predict the pixel values for shares. Figure 1.3 shows possible combination of shares for 2-out-of-2 scheme. The first row in Figure 1.3 shows possible basis matrices













Pixel	Share 1	Share 2	Share 1+ Share2
□	 	 	 
■	 	 	 

Figure 1.3: Shares generated for white/black pixel using basis matrices given in Equation 1.4. First column indicates white/black pixel, column two and third indicates visual representation of share 1 and share 2, and last column indicates OR of column two and three

for white pixel to generate shares and second row for black pixel.

The relative difference (α) of the 2-out-of-2 scheme is computed using Equation 1.1 as $\frac{1}{2}$. To ensure the better visual quality, the contrast must be equal to or greater than 1 for human visual system. Here pixel expansion (m) is considered as 2. Using equation 1.2 the contrast (β) for the 2-out-of-2 VCS is computed as 1.

Figure 1.4 shows the sample shares generated for 2-out-of-2 scheme. Figure 1.4 (a) shows the input secret image, the shares in Figure 1.4 (b) and (c) are generated using basis VCS model, Figure 1.4 (d) shows the output image recovered after stacking shares. As observed from Figure 1.4 the above scheme suffers from the problem of expansion of image in horizontal or vertical direction. Using horizontal layout, if input image has size $n \times n$, then it becomes of size $n \times 2n$ after stacking shares.

1.3 MOTIVATION

There exists many visual cryptography techniques to securely transmit visual media over the network. Still, the VSS scheme suffers from common problems as discussed

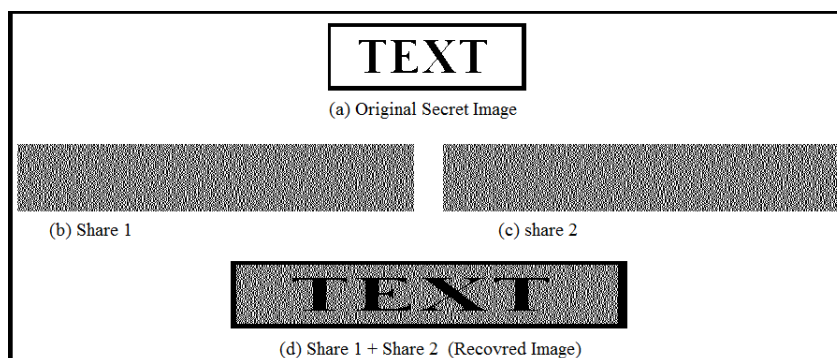


Figure 1.4: Sample output of the 2-out-of-2 VCS (a) Original secret image, (b) generated Share 1, (c) generated shares 2, and (d) output image after stacking share 1 and share 2 together using simple 'OR' operation

below.

- Majority of the techniques recover secret image with poor contrast. It is observed that the maximum contrast achievable by VSS techniques is 50%. Hence there is a need to propose a technique to improve the contrast of secret image.
- The VSS was proposed for binary images. VSS mainly converts gray-scale and color image into monotone images using halftone techniques. Recovered image in VSS is always a monotone image. Hence there is a need to recover multitone image in same format.
- **Underwater images:** Analysis of underwater image is an emerging field in ocean engineering. Ocean engineering tries to analyze underwater images for biological and sediment particles. The underwater images are different than natural images. They have degraded quality due to effect of scatters and absorption property of water. They suffer from low contrast and color distortion problem. As underwater images are used for discovering biological and sediment particles, transmitting them securely with good quality is an emerging area of research. In underwater observation, presence of floating particle makes it difficult to capture clear and turbid free images, which leads to poor visibility of images. Due to importance of underwater resources, there is need to transmit images securely and with maximum visibility.

- **Medical images:** Now a days due to availability of the Internet medical information is being shared over the communication networks due to ease of technology. The patient's medical information has to be securely communicated over the network for automatic diagnosis. Most of the communication networks are prone to attacks from an intruder thus compromising the security of patients data. Therefore, there is a need to transmit medical images securely over the network.

This thesis aims to address the above limitations of VSS with an efficient model resulting in better reconstruction contrast for gray-scale and color images.

1.4 THESIS CONTRIBUTIONS

To improve the visual reconstruction quality of the Secret Image (SI), this thesis presents various VSS based Schemes. The thesis concentrates on recovery of the SI in the multitone format while retaining maximum visual quality.

1. Presented a BPVSS based VSS scheme termed as Randomized VSS (RVSS) (Mhala et al. 2018). RVSS scheme embeds original pixel values into the shares. To embed the pixel values first transform the shares into frequency domain using Discrete Cosine Transform (DCT). Once shares are transformed into frequency domain, embed the pixel information into shares. At the receiver end extract the embedded pixel and use it to improve visual reconstruction quality of the SI.
2. Presented a novel super-resolution based progressive VSS scheme (Mhala and Pais 2019a) to transmit SI securely over the network. The scheme improves the contrast and the visual quality of the SI by using super-resolution technique.
3. The efficiency and effectiveness of the presented schemes to transmit SI over the network are tested on the underwater and histopathological images (Mhala and Pais 2019b).
4. A CNN-based architecture is also presented in the thesis to reduce various artifacts present in the reconstructed image (Mhala and Pais 2020). Proposed a CNN architecture that uses an extracted residual image learned from the SI to further improve the visual quality of the SI.

1.5 THESIS ORGANIZATION

The rest of the thesis is organized as follows:

- **Chapter 2 : Literature review:** This chapter presents basic Visual secret sharing model followed by an overview of the research work carried out by researchers in the field of visual cryptography.
- **Chapter 3 : Randomized Visual Secret Sharing (RVSS) scheme for gray-scale and color images :** This chapter presents a Randomized Visual Secret Sharing (RVSS) scheme for gray-scale and color images.
- **Chapter 4 : Contrast enhancement of Progressive Visual Secret Sharing (PVSS) scheme for gray-scale and color images using super-resolution:** This chapter presents a Super-Resolution based Visual Secret Sharing (SRVSS) scheme for gray-scale and color images.
- **Chapter 5 : Applications of the Visual Cryptography:** This chapter describes the applications of visual cryptography to transmit complex medical images for computer aided diagnosis and underwater images over a network.
- **Chapter 6: Conclusions and future scope:** The chapter concludes all the presented techniques of this thesis and provides some recommendations for the future research directions.

CHAPTER 2

LITERATURE REVIEW

A substantial amount of work has been done to propose a Visual Secret Sharing (VSS) scheme in the field of visual cryptography. This chapter categorized VSS schemes into two main types based on the recovery of secret image as:

- Traditional Visual Secret Sharing Schemes.
- Progressive Visual Secret Sharing Schemes.

This Chapter presents an example of basic 2-out-of-2 VSS model with similar pixel expansion along horizontal and vertical direction, followed by different types of VSS schemes developed so far. Further, the literature survey is organized into four sections, Section 2.1 presents a discussion on traditional visual secret sharing schemes. The Progressive Visual Secret Sharing (PVSS) Schemes are presented in Section 2.2. Section 2.3 discusses the work done in the field of reversible data hiding techniques. Finally, Section 2.4 discusses the recent techniques studied in the area of Super-Resolution.

2.1 TRADITIONAL VISUAL SECRET SHARING SCHEMES

In traditional secret sharing scheme, to recover an image at least k shares out of n shares need to be stacked together. This concept also referred as “All or nothing” recovery scheme. The idea of visual cryptography was introduced by Naor and Shamir (1994a). Their technique is based on “All or nothing” recovery scheme, in which users stack defined minimum number of shares to reveal secret. This scheme is also known

Pixel	Share 1	Share 2	Share 1 + Share 2
□			
■			

Figure 2.1: Basis matrices for 2 out of 2 scheme ($m=4$). First column indicates white/black pixel, column two and three indicates visual representation of share 1 and share 2, and last column indicates OR of column two and three

as threshold scheme. Figure 2.1 shows basis matrices used for generating shares ($m=4$). Let us consider a pixel expansion ratio as 4. It means for each pixel of secret image, generate four pixel combination in shares. Figure 2.1 visually shows that white/black pixel can be replaced with one of the patterns. The first row shows the possible combination of basis matrices for white pixel. To ensure imperceptible generation of shares, randomly select one of the combination out of six possibilities. Generating shares by selecting random pattern makes scheme secure. Figure 2.2 shows an example of the VCS that has been generated with pixel expansion ($m=4$) by Naor and Shamir (1994a). The original secret image having word 'TEXT' written is shown in Figure 2.2 (a). Figure 2.2 (b-c) shows the shares generated for the secret image 'TEXT' and recovered image after stacking share 1 and 2 together using 'OR' operation is shown in Figure 2.2 (d). It is noticeable that VCS provides simple and secure solution to protect visual information.

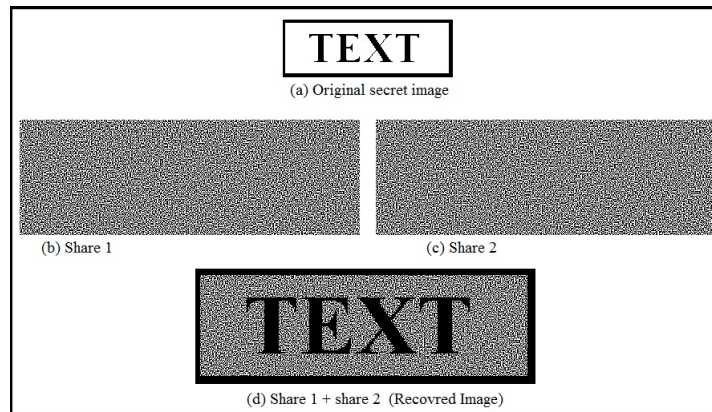


Figure 2.2: A sample example for 2 out of 2 scheme ($m=4$). (a) Original secret image, (b) generated Share 1, (c) generated shares 2, and (d) output image after stacking share 1 and share 2 together using simple 'OR' operation

The VSS scheme proposed by [Naor and Shamir \(1994a\)](#) is uniform in nature. It means any k users out of n were able to recover the secret image. [Ateniese et al. \(1996\)](#) proposed more general VSS scheme known as General Access Structure (GAS). It is more sophisticated way of generating shares. In their work they have divided users into two sets as qualified and forbidden. The qualified users will be considered as key users to recover secret. The secret will be revealed only if it contains share of qualified users. The forbidden users alone cannot recover the secret, hence making the scheme more secure. The shares generated using above scheme had noise-like appearance. [Ateniese et al. \(2001\)](#) extended VSS work by proposing a scheme to generate meaningful shares known as Extended Visual Cryptography Scheme (EVCS).

Extended Visual Cryptography Scheme (EVCS), permits the construction of VSS scheme which generates meaningful shares as opposed to noise-like shares. To recover the secret image, whenever set of qualified users stack their shares together, meaningful information disappears and secret is recovered. By adding some meaningful cover image on shares it makes share less suspicious. EVCS assigns visually distinct shares to n users. The Figure [2.3](#) shows the sample of shares generated using EVCS. Figure [2.3\(a\)](#) shows secret image that need to be encrypted. In Figure [2.3](#) (b-d) there are three shares generated having letter A, B and C as cover images. Visual Cryptography Scheme (VCS) shown in Figure [2.3](#) recovers secret image by stacking 2 out of 3 shares. It is

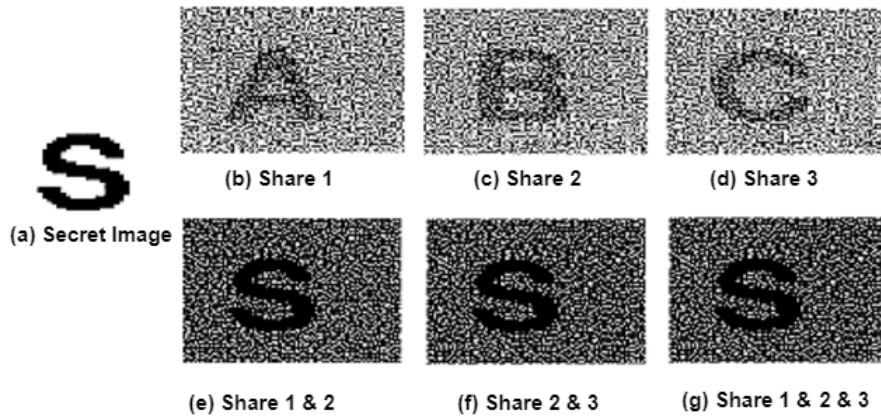


Figure 2.3: Shares generated using EVCS (a) secret image, (b-d) shares generated with meaningful cover image, (e) output after stacking share 1 and 2 together, (f) output after stacking share 2 and 3 together and (g) output of EVCS after stacking share1, 2 and 3 together

noticeable from Figure 2.3 (e-g) that meaningful shares are getting fade away to recover secret image.

Ito et al. (1999) proposed image size invariant visual cryptography. The visual cryptography schemes discussed previously were able to generate shares having increased share size. The techniques used by above VCS are based on pixel expansion. Generating shares with expanded shares has disadvantage like, (i) As shares are having increased size it leads to wastage of storage. (ii) It suffers from high consumption of bandwidth while transmitting shares over the network. (iii) Generated shares are distorted due to increase in size of shares. The method proposed by Ito et al. (1999) removes the need for pixel expansion. It recovers secret image with same size as of original image. But the method suffers from poor contrast problem. Figure 2.4 shows the sample of size invariant recovery of original image. Figure 2.4 (a) shows the secret image, followed by recovered image using 2 out of 3 VSS scheme and Figure 2.4 (c) shows the output image of the 3 out of 3 stacking method. It is evident from images that, sizes of the recovered images are same and no pixel expansion has been used to recover secret image. Also it can be observed that, for less participant it suffers from problem of poor contrast.

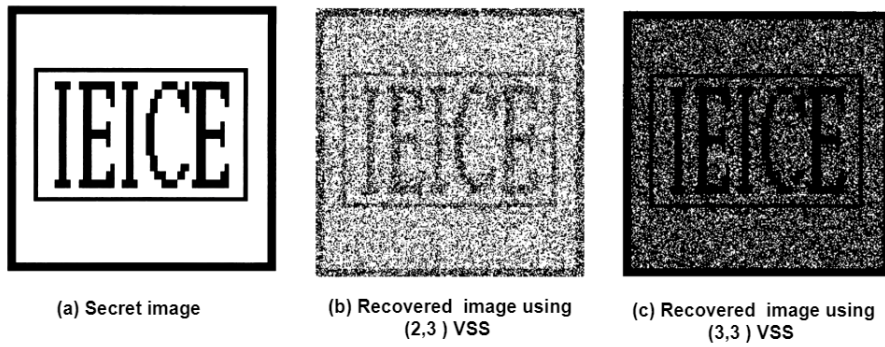


Figure 2.4: Size invariant shares generation using Ito et al. (1999)'s scheme. (a) Original secret image, (b) recovered secret image using (2,3) VSS, and (c) recovered secret image using all (3,3) shares

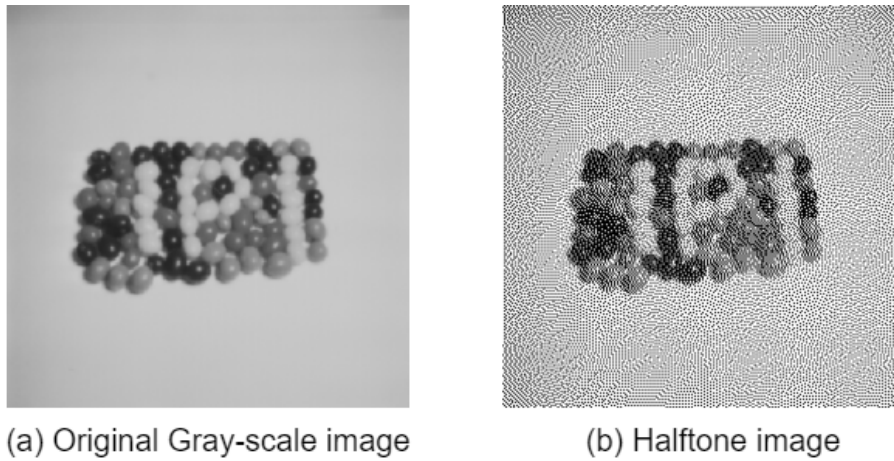


Figure 2.5: An example of Halftone technique. (a) the original image, and (b) Halftone image generated for original image

2.1.1 VSS for gray level images

VSS schemes discussed above works on the binary images. It is today's need that one should be able to encrypt gray-level images instead of binary images. Many researchers proposed gray-level visual cryptography based on halftone technology (Lin and Tsai 2003; Ulichney 1999). The halftone is the photographic technique that simulates continuous tone imagery through the use of dots, varying either in size or in spacing, thus generating a gradient-like effect. Halftone technique uses density of dots to represent gray image so that human visual system can perceive continuous gray image. The halftone technology has been used by printing industries to save the cost of printing.

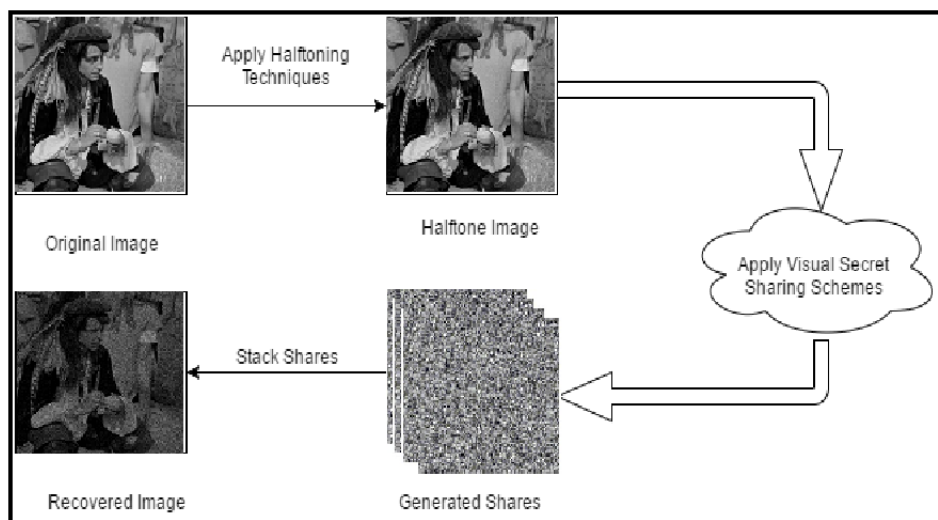


Figure 2.6: Overview of the gray-scale VSS system based on halftone technology

Figure 2.5 shows an example of halftone image. From Figure 2.5 it is noticeable that the converted halftone image looks visually similar to original image. It visually retains the gray level appearance of the image.

Many researchers (Blundo et al. 2000; Lin and Tsai 2003; MacPherson 2002; Ulichney 1999; Zhou et al. 2006a) have proposed halftone visual cryptography scheme based on halftone technology. Wang et al. (2009) proposed gray level VSS using halftoning via error diffusion. Error diffusion is less complex algorithm to generate halftone image from gray-scale image. Error diffusion mainly consists of two components. First component is thresholding block which outputs binary value for a gray pixel based on threshold. The threshold defined by block can depend on position of pixel. Second component filters the quantization error at each pixel using various technique like Floyd-Steinberg (Floyd 1976) error filter and is diffused to other pixel to set future pixel of an image. Figure 2.6 shows the system flow for generating shares for gray-scale images.

The use of halftone technique makes it possible to directly apply existing binary image VSS scheme for gray-level images. The different gray-level visual cryptography schemes are also studied by authors in (Blundo et al. (2000); Iwamoto and Yamamoto (2002); MacPherson (2002); Yang and Chen (2005)).

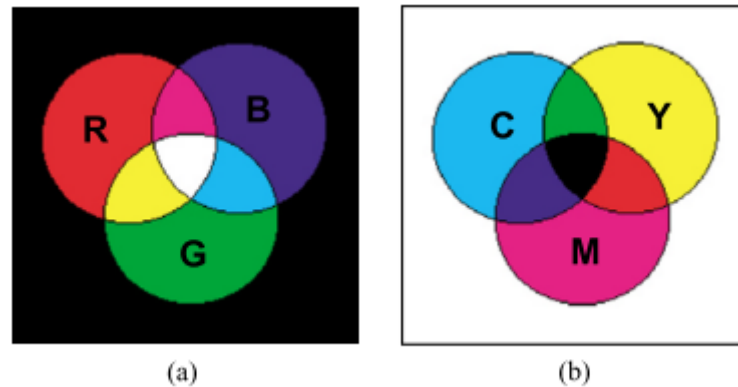


Figure 2.7: General color model used for VSS. (a) Additive color model, (b) Subtractive color model

2.1.2 VSS for color images

Nowadays due to advancement in technology use of color images are becoming need of time. Many authors proposed visual cryptography technique for color images. Figure 2.7 shows two popular models namely additive and subtractive associated with color images. The primitive colors in additive model are red, green and blue. Combining red, green and blue colors together it results into white color. The computer monitor mainly uses additive color models. Rijmen (1996) proposed color cryptography based on additive model. They used red, green, blue and white (transparent) colors to generate shares. But with addition of any color into white becomes white color in additive model. Figure 2.7 (b) shows subtractive model. Subtractive model is being used by color printers. The model contains cyan, magenta and yellow as primitive color. The subtractive model works on principal of reflection. The light incident on surface gets reflected back in subtractive model which is perceived by Human Visual System. For example in case of apple, it appears to be red. The apple absorbs green and blue part of the light and reflects red light, hence providing red color appearance to human eye.

Hou (2003) proposed color visual sharing scheme based on subtractive model. Subtractive model mainly being used by printing media. Visual cryptography generates shares which can be printed on transparency. As subtractive model is more suitable for visual cryptography Hou (2003) used this model and proposed color visual sharing

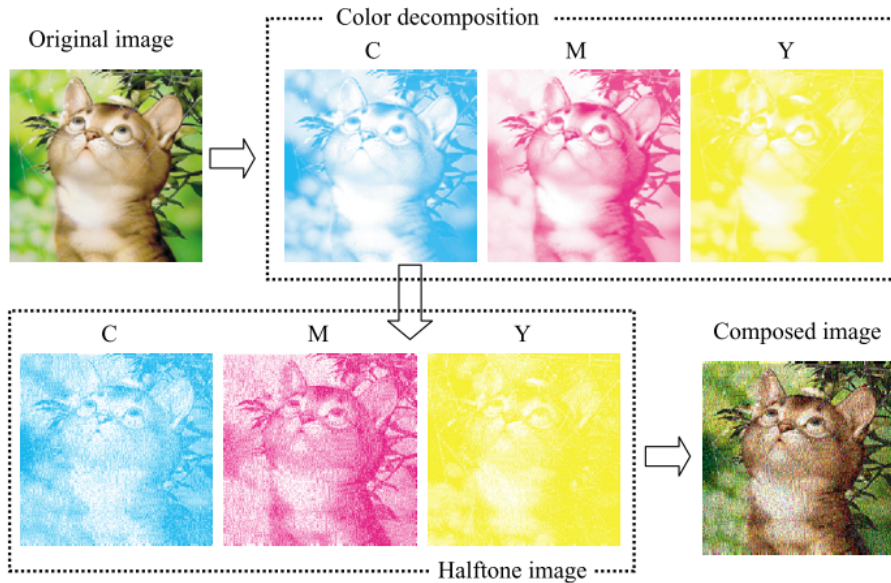


Figure 2.8: Color image visual cryptography (Hou 2003) example using CMY color model

scheme. Hou (2003) used concept of halftone to generate shares. Figure 2.8 shows the overview of the system proposed by Hou (2003). To apply VSS scheme on color images, first convert RGB image into CMY model, then apply halftone on each color channel as shown in Figure 2.8. Once the halftone color images are formed then traditional VSS schemes on each channel is applied to generate shares. The final composed image after applying halftone on each channel is shown in Figure 2.8.

2.2 PROGRESSIVE VISUAL SECRET SHARING SCHEMES

Although traditional visual secret sharing scheme allows sharing of secret information, it suffers from pixel expansion problem. In pixel expansion, image will be expanded by a factor of m ($m \geq 2$). This pixel expansion leads to the wastage of storage and also consumes more transmission bandwidth. Traditional visual secret sharing also suffers from problem of poor contrast. Progressive Visual Secret Sharing (PVSS) schemes solves the problem of pixel expansion and poor contrast as discussed above. Traditional visual secret sharing scheme works on principal of “All or nothing”. Whereas PVSS gradually reveals secret image. PVSS can be categorized into two, based on recovery method as: (i) Recovering entire image gradually (Chen 2009a; Fang 2008a; Fang and

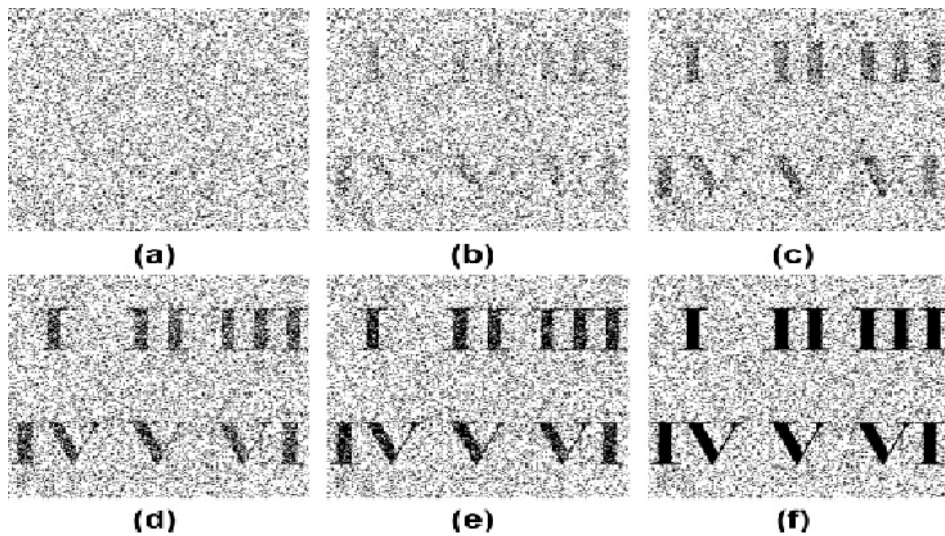


Figure 2.9: PVSS: Recovering entire image gradually. (a) share 1 (b) stacked share 1 and share 2 (c) stacked shares 1- 3, (d) Stacked shares 1-4, (e) stacked shares 1-5, and (f) output of all the shares stacked together

Lin [2006a]; Hou and Quan [2011a) and (ii) Recovering a parts of image gradually (i.e. block by block recovery of image) (Wang [2009a]; Wang et al. [2007a). The first category considers secret image as a whole image to recover. Stacking of more than one share recovers secret image but it should be noted that contrast of the secret image gets better and better with the stacking of more shares. Figure 2.9 shows the recovery of secret using six participants. It can be observed from the PVSS schemes that minimum two share holder can also able to recover secret, but it will have poor contrast. The contrast gets gradually better and better with the involvement of more participants. Figure 2.9 (f) appears to be more visible than (b). The second category recovers image block by block. Wang et al. [2007a) and Wang [2009a) proposed block based sharing schemes, which reveal secret properly but they suffer from some common defects like:-

- Due to irregularities in generating sharing matrices, it limits the number of participants.
- The use of pixel expansion causes generation of shares to be larger than secret image.
- The contrast of recovered image decreases as number of participant increases.
- These schemes are not suitable for gray-level and color images.

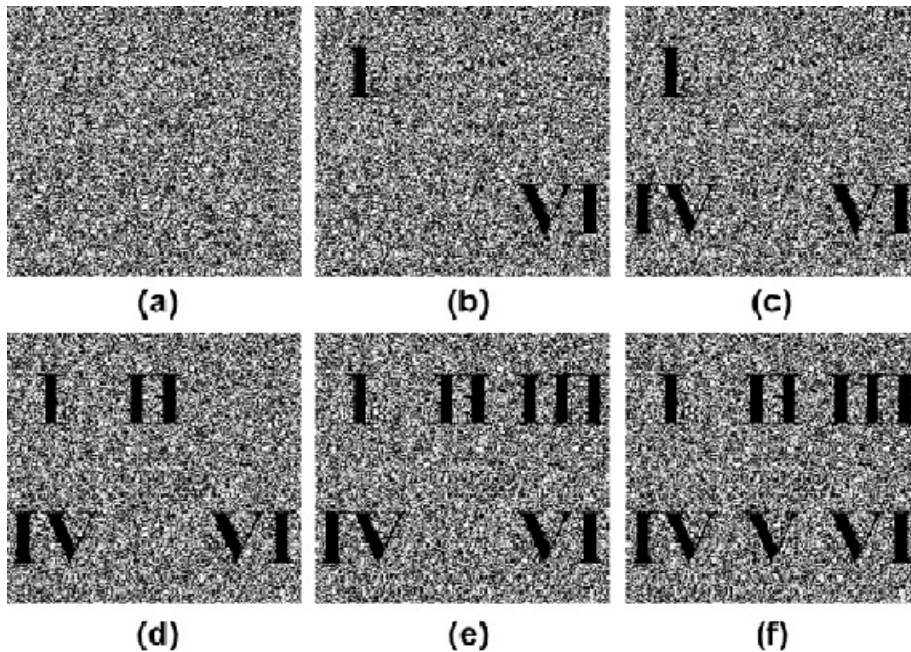


Figure 2.10: PVSS: Recovering secret image block by block . (a) share 1 (b) stacked share 1 and share 2 (c) stacked shares 1- 3, (d) Stacked shares 1-4, (e) stacked shares 1-5, and (f) output of all the shares stacked together

[Hou et al. \(2013b\)](#) proposed block based visual sharing scheme which handles all the mentioned problems. They proposed non-expanded, block based recovery model namely Block-based Progressive Visual Secret Sharing (BPVSS). BPVSS mainly works like jigsaw puzzle. After joining all pieces together, secret image gets revealed. Every share generated using BPVSS works like a sub image of a secret image. To recover the secret image we have to rely on all the participants. In addition to that, BPVSS maintains 50% contrast regardless of number of share stacked. BPVSS is more suitable for complex images, like gray-level and color images. BPVSS generates shares of same size, hence recovers secret image of same size as that of original image. [Figure 2.10](#) shows the block based recovery of the secret image.

[Table 2.1](#) summarizes the different techniques developed so far in the field of VSS. [Table 2.1](#) classified various methods based on share type, pixel expansion, recovery type, and type of secret along with output image (i.e. halftone or multitone). As it is observed all of the discussed techniques produce halftone image as output. The recovered image using above technique always results in the binary image (monotone).

Table 2.1: Overview of visual secret sharing schemes

Method	Pixel expansion	Share Type (Noise-like/Meaningful)	Recovery Type	Type of secret Image	Type of output image
Naor and Shamir (1994b)	Yes	Noise-like	All or nothing	Halftone	Halftone
Ateniese et al. (1996)	Yes	Noise-like	All or nothing	Halftone	Halftone
Ateniese et al. (2001)	Yes	Meaningful	All or nothing	Halftone	Halftone
Zhou et al. (2006a)	Yes	Meaningful	All or nothing	Halftone	Halftone
Fang (2008a)	Yes	Meaningful	Progressive	Halftone	Halftone
Wang et al. (2009)	Yes	Meaningful	All or nothing	Halftone	Halftone
Hou et al. (2013b)	No	Both	Progressive	Halftone	Halftone
Hou et al. (2014)	No	Both	All or nothing	Halftone	Halftone
Hou and Quan (2011a)	Yes	Noise-like	Progressive	Halftone	Halftone

Which motivates to solve the problem of recovery of secret image in the halftone format. Finally, Table 2.2 summarizes all discussed techniques in the field of VSS. Table 2.2 briefs advantages and disadvantages of a method. From Table 2.2 it is observed that, contrast is the major problem associated with recovery of secret image.

Recently, Zheng et al. (2020) proposed generative adversarial networks (GANs) based key secret sharing scheme in block-chain. The author used GAN concept to generate multiple non-progressive shares. They have first divided the original image into original sub-images using segmentation. Next they have encoded each original sub-image by DNA coding. Finally they have trained the proposed network to find the key secret sharing results. Cheng et al. (2018) proposed improved visual secret sharing scheme for QR code applications. The scheme uses (k,n) access structure to solve the QR encoding and decoding at receiver side using XOR operations.

Further many applications also has been proposed by researchers using VSS schemes. Like using VSS, biometric templates have been protected for various traits (Chin et al. 2006; Divya and Surya 2012; Monoth et al. 2010; Revenkar et al. 2010; Ross and Othman 2010). In Chin et al. (2006); Revenkar et al. (2010); Sinduja et al. (2012), authors introduced VSS scheme for iris template protection, Ross and Othman (2010) for the face template protection, Divya and Surya (2012) for the palm print template protection and Monoth et al. (2010) for fingerprint template protection. In Monoth et al. (2010), authors adopted a $(2, 2)$ basic VSS scheme for encrypting the secret fingerprint image. Shares generated using this method are deposited in two separate databases. In Kaur and Khanna (2016), authors summarized the existing works in cancelable biometrics and VSS for protecting biometric templates. In Kumar et al. (2020), authors generated a cancelable biometric template using VSS and $n - 1$ cover images. They used three different combinations for generating the shares. 1. One secret biometric image and $n - 1$ random cover images, 2. One secret biometric image and $n - 1$ permuted biometric images as cover images, and 3. Both secret and cover images are random permuted biometric images.

Table 2.2: Pros and Cons of Visual Secret Sharing (VSS) schemes

Method	Pros	Cons
Naor and Shamir (1994b)	<ul style="list-style-type: none"> - It is easy to implement. - The secret image can be perceived by HVS - It doesn't require any keys to recover secret image. 	<ul style="list-style-type: none"> - Generates uniform shares for each participant. - Generates noise-like shares. - Suffers from problem of pixel expansion.
Ateniese et al. (1996)	<ul style="list-style-type: none"> - Provides GAS for k-out-of-n sharing scheme. - We can divide users into two sets as authenticated and forbidden, which makes scheme more secure. 	<ul style="list-style-type: none"> - Suffers from problem of pixel expansion. - Generates noise-like shares and cannot generate shares for gray-scale and color images
Ateniese et al. (2001)	<ul style="list-style-type: none"> - Generates meaningful shares. 	<ul style="list-style-type: none"> - Suffers from problem of pixel expansion.
Zhou et al. (2006a)	<ul style="list-style-type: none"> - Generates shares for gray-scale image. - Provides meaningful shares to each user. 	<ul style="list-style-type: none"> - Suffers from problem of cross interference of shares while recovering secret image.
Fang (2008a)	<ul style="list-style-type: none"> - Provides progressive recovery of secret image. - Generates meaningful shares for gray-scale image. 	<ul style="list-style-type: none"> - Suffers from problem of pixel expansion. Cannot generate shares for color images.
Wang et al. (2009)	<ul style="list-style-type: none"> - Provides recovery of shares without any cross interference between shares and generates shares for gray-scale images. 	<ul style="list-style-type: none"> - Suffers from problem of pixel expansion and cannot generate shares for color images.
Hou and Quan (2011a)	<ul style="list-style-type: none"> - Generates progressive shares and non-expanded shares. - Recovers secret image gradually with better contrast. 	<ul style="list-style-type: none"> - Generates noise-like shares. - Provides the contrast of $(n - 1)/n$ for n participants.
Hou et al. (2013b)	<ul style="list-style-type: none"> - Generates non-expanded shares for both gray-scale and color image. 	<ul style="list-style-type: none"> - Recovers secret image as monotone image. - Provides maximum contrast upto 50%.
Hou et al. (2014)	<ul style="list-style-type: none"> - Provides share recovery with various contrast levels. - Generates non-expanded shares 	<ul style="list-style-type: none"> - Generates noise-like shares. - Recovers image using "All or nothing" methodology.

2.3 REVERSIBLE DATA HIDING TECHNIQUES

This subsection, presents various techniques proposed by researchers in the field of reversible data hiding. The proposed work, mainly focusing on the gray-scale and color images. This section considers the work carried out by researchers pertaining to gray-scale and color images in the field of data hiding. The data hiding technique proposed by [Chang et al. \(2007\)](#) focuses on hiding data in frequency domain. The scheme makes use of Human Visual System (HVS). The HVS is more sensitive towards the low and middle frequency. The small change in low and mid frequency remains imperceptible by HVS. [Chang et al. \(2007\)](#) proposed a technique to hide data into frequency domain. They have transformed the image from spatial domain to frequency domain using Discrete Cosine Transform (DCT). Then the embedding is done in the middle frequency of the image.

Data hiding has the suitable applications in the area of military, medical and many more. The technique which restores the original image after extracting the hidden information from the transformed image is termed as reversible data hiding. [Iwata et al. \(2004\)](#) proposed the reversible data hiding technique which makes use of ceaseless zeros to embed the data. They have transformed the image from spatial domain to frequency domain using DCT. They quantize the DCT coefficient using modified quantization table. Which generates more ceaseless zeros in the transformed image. They have used middle frequency location having ceaseless zeros to hide data into image.

Further, [Gujjunoori and Amberker \(2013a\)](#) and [Gujjunoori and Amberker \(2013b\)](#) proposed reversible data hiding technique similar to [Chang et al. \(2002\)](#) to hide data in videos. They have embedded the data in the middle frequency. They achieved the embedding capacity of 3 bit for each of the sets. Further RVSS scheme proposed by [Mhala et al. \(2018\)](#) modified the data hiding scheme given in [Gujjunoori and Amberker \(2013a,b\)](#) to work with images. They have modified data hiding scheme to embed pixel data into shares. The techniques presented in this thesis mainly use the concept of reversible data embedding into images to improve the contrast of the image.

2.4 SUPER RESOLUTION

Super-resolution (SR) is the process of obtaining one or more high-resolution images from one or more Low-resolution (LR) observations, has been a very attractive research topic over the last two decades. It has practical applications in many real-world problems in different fields, such as satellite and aerial imaging, medical image processing, facial image analysis, text image analysis, sign and number plates reading, etc. Many researchers developed a new super resolution technique to address specific area. Super-Resolution techniques can be categorized as (i) Multiple Image Super-Resolution (MISR), and (ii) Single Image Super-Resolution (SISR).

2.4.1 Multiple Image Super Resolution

Multiple image (or classical) SR algorithms are mostly reconstruction-based algorithms, i.e., they try to address the aliasing artifacts which is present in observed LR images due to under-sampling process by simulating the image formation model. [Tsai \(1984\)](#) first proposed idea of super resolution. They observed that, single scene image restoration is possible from multiple down-sampled version of a scene. For this purpose they used frequency domain model to super resolve the image. A different approach was proposed by [Irani and Peleg \(1991, 1993\)](#) based on Iterative Back Projection (IBP) method. This method starts with initial guess of the output image. The initial guess is improved with each iteration until solution converges or reaches maximum iteration. Basically they have tried to optimize the initial guess by minimizing error between computed and initial image.

[Joshi et al. \(2005\)](#) proposed the multiple image super resolution based on zoomed observation. They found out that zoomed observation can be used as cue to super resolve the image. The most zoomed observation contains detailed information about the scene. Whereas least zoom observation covers the entire region with least details. [Joshi et al. \(2005\)](#) used this property of an image. They had captured the zoomed observation of a scene and proposed zoom based super resolution technique.

2.4.2 Single Image Super Resolution (SISR)

In Single image Super Resolution (SISR) method authors try to recover High-Resolution (HR) image from single LR image. In [Nasrollahi and Moeslund \(2014\)](#), authors categorized SISR into three categories as (i) Interpolation based SR (ii) Reconstruction based SR (iii) Learning based SR. In Interpolation based SR, LR image is interpolated using popular image interpolation techniques (bilinear, bicubic, and Lanczos) to generate HR image. These techniques are better for smooth region as they compute weighted averaging of neighboring pixel. The smooth region has the property that they are similar in appearance, so HR recovery using interpolation is good for such images. But high frequency component like edges, corners present in image gets lost due to interpolation.

In Reconstruction based SR, HR image is reconstructed using similar LR image patches. The method tries to solve the ill posed SR problem by exploring self similarity between LR image to construct HR image. Although these techniques are popular in multiple image in SISR it suffers from problem of ill conditioned image registration due to less number of LR observations. ([Ogawa et al. 2012](#); [Sun et al. 2008, 2011](#); [Yang et al. 2012b](#)) these are few techniques among many available reconstruction based SR.

The learning based SR, makes use of training images to learn about scene. The performance of the method depends on the efficient learning model used. The method tries to learn the correlation between LR and the learned parameters to recover SR images. Recently, [Dong et al. \(2016\)](#) proposed SISR method based on deep convolution networks. The method learns end-to-end mapping between the low/high resolution images. To reconstruct SR image [Dong et al. \(2016\)](#) first extracts patches from LR image and represents it as high dimensional vector. Once patches are extracted non linearly map this vector onto another high dimensional vector. Finally, reconstruct the SR image by aggregating all high dimensional vectors. Many authors also proposed SISR techniques based on learning method ([Rohit et al. 2017](#); [Yang et al. 2012a, 2010](#)).

2.5 PROBLEM DESCRIPTION

In the field of visual cryptography, different mechanisms like visual secret sharing with pixel expansion, without pixel expansion and progressive block based methods have

been developed over past years. Although BPVSS is a good approach suitable for gray-scale and color images, but restored image after joining all shares results in a binary image. Also contrast of the restored image is restricted to 50% and 25% for noise-like and meaningful shares respectively. Hence there is need to develop better VSS scheme with improved contrast.

2.6 PROBLEM STATEMENT

Design and analysis of visual secret sharing scheme with an improved contrast for gray-scale and color images.

2.7 OBJECTIVES

- Propose a BPVSS based scheme to improve the contrast of the recovered image (gray-scale and color) by embedding data into shares.
- Propose a BPVSS based scheme to further improve quality of the recovered image using Super-Resolution techniques.
- Design and apply BPVSS based scheme to transmit underwater images.

2.8 SUMMARY

Visual cryptography is a technique which secures visual information. It is very useful technique as decryption can be done using Human Visual System. The literature survey on many visual cryptography techniques are presented in this chapter. The methods discussed in this chapter suffers from the common drawbacks like expansion of recovered image, restriction on number of users, recovery of multi-tone image as binary image, etc. The BPVSS scheme tries to solve the many drawbacks, but it also suffers from common problems like, the BPVSS technique provides contrast of at-most 50% for gray-level images and 25% for color images. Also, BPVSS recovers the monotone image as output for multi-tone image. Hence there is a need to develop a better VSS scheme with improved contrast for gray-scale and color images. The research work carried out by various researchers in the field of data hiding and super-resolution are also discussed in this chapter. This chapter formulates the problem statement and also

2. Literature Review

provides the objectives achieved by this thesis.

CHAPTER 3

RANDOMIZED VISUAL SECRET SHARING (RVSS) SCHEME

The concept of Visual Secret Sharing (VSS) scheme is basically designed to share visual information over the communication network. Compared with other traditional encryption/decryption processes, VSS scheme has the advantage of using Human Visual System (HVS) to decrypt the secret images without any complex mathematical computations. In the VSS scheme, secret image is first divided into n random shares. After joining at least k (or more) shares, the secret image gets restored, otherwise restoration of the secret image becomes impossible. VSS is also referred as (k, n) threshold scheme, due to properties of stacking k out of n shares to reveal the secret image. This chapter proposed a Randomized Visual Secret Sharing (RVSS) scheme for gray-scale and color images. The chapter first generates block-based shares and then embeds random pixel values in to shares. Further these embedded information is used to improve the contrast and visual quality of the secret image.

Although the threshold scheme proposed by [Naor and Shamir \(1994a\)](#) is the first step towards the future of visual cryptography, this method has many drawbacks. This scheme uses pixel expansion method for the generation of shares which lead to wastage of storage, distortion of an image, and more consumption of transmission bandwidth. To resolve these issues, another secret sharing method named as Progressive Visual Secret sharing (PVSS) was introduced by [Chen \(2009b\)](#); [Fang \(2008b\)](#); [Fang and Lin \(2006b\)](#); [Hou and Quan \(2011b\)](#). This scheme uses multiple sharing matrices for black

3. Randomized Visual Secret Sharing (RVSS) Scheme

and white pixels to generate shares of the secret image without any pixel expansion (the secret image and the shares are of the same size). The secret image is restored progressively by joining all the shares.

Progressive VSS uses two methods to generate shares of the secret image. The first method proposed by [Chen \(2009b\)](#); [Fang \(2008b\)](#); [Fang and Lin \(2006b\)](#); [Hou and Quan \(2011b\)](#) considers the secret image as a whole to generate the shares. On the other hand, the second method proposed by [Wang \(2009b\)](#); [Wang et al. \(2007b\)](#) divides the secret image into non-overlapping blocks which contain the information related to the secret image. Superimposition of any two shares reveals the related blocks of the secret image. So, the secret image gets progressively restored block by block.

Block-based Progressive Visual Secret Sharing (BPVSS) scheme is an effective technique for sharing secret images. This method has the following advantages:

(i) It does not impose any bound on the number of members. (ii) It gives contrast up to 50% for noise-like shares and 25% for meaningful shares. (iii) It does not use pixel expansion method so that shares and secret image, both are of the same size. (iv) This method can be applied on gray-scale as well as color images.

Although BPVSS scheme restores the secret image with good contrast (50% and 25% for noise-like and meaningful shares respectively), it has few drawbacks. The reconstructed image always results in a binary image and the quality is poor (i.e. maximum 50% contrast). Hence there is a need for improvement in the contrast of the reconstructed secret image. A novel technique known as RVSS for improving the contrast of the reconstructed image to 70-90% in case of noise-like and 70-80% for meaningful shares is presented in this chapter.

Rest of the chapter is organized as follows: The Section [3.1](#), briefs about the proposed Randomized Visual Secret Sharing (RVSS) scheme for gray-scale and color images. Experimental results are provided in Section [3.2](#), finally, Section [3.3](#) concludes the chapter.

3.1 RANDOMIZED VISUAL SECRET SHARING (RVSS) SCHEME

The proposed Randomized Visual Secret Sharing (RVSS) (Mhala et al. 2018) technique makes use of BPVSS scheme for secret share generation and Discrete Cosine Transformation (DCT) based reversible data hiding technique for hiding the additional information about pixels into shares. RVSS scheme comprises of four steps as follows: (i) Generation of the shares, (ii) Embedding the secret information into shares, (iii) Extraction and reconstruction of secret image, and (iv) Embedding data back into the restored image and apply post-processing (i.e. Remove random noise using Wiener filter). Figure 3.1 shows overview of the RVSS system. All the four steps mentioned above are shown in the Figure 3.1 with a sample gray-scale image (clock.tiff) as an input Secret Image (SI). The different steps of the RVSS system are explained below.

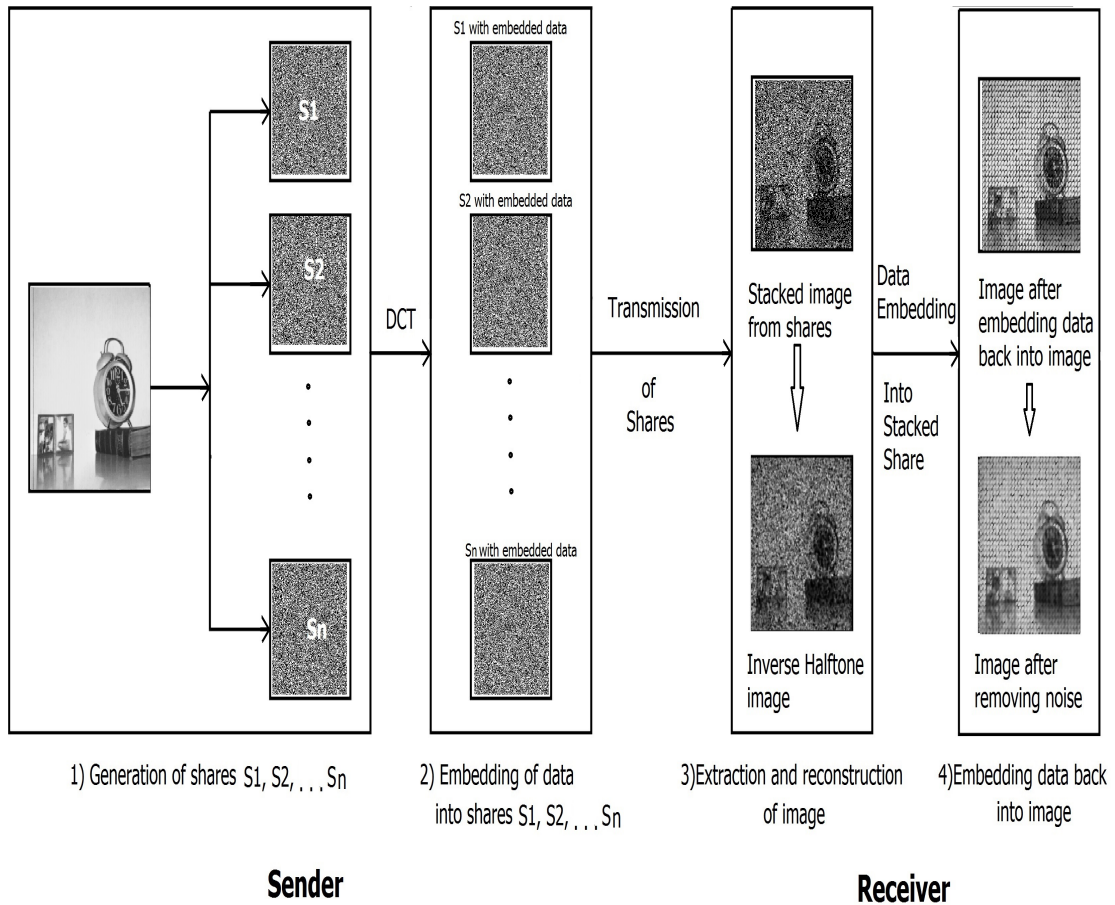


Figure 3.1: Overview of the RVSS (Mhala et al. 2018) system. 1) Generation of shares S_1, S_2, \dots, S_n , 2) Embedding of data into shares S_1, S_2, \dots, S_n , 3) Extraction and reconstruction of image, 4) embedding data back into shares

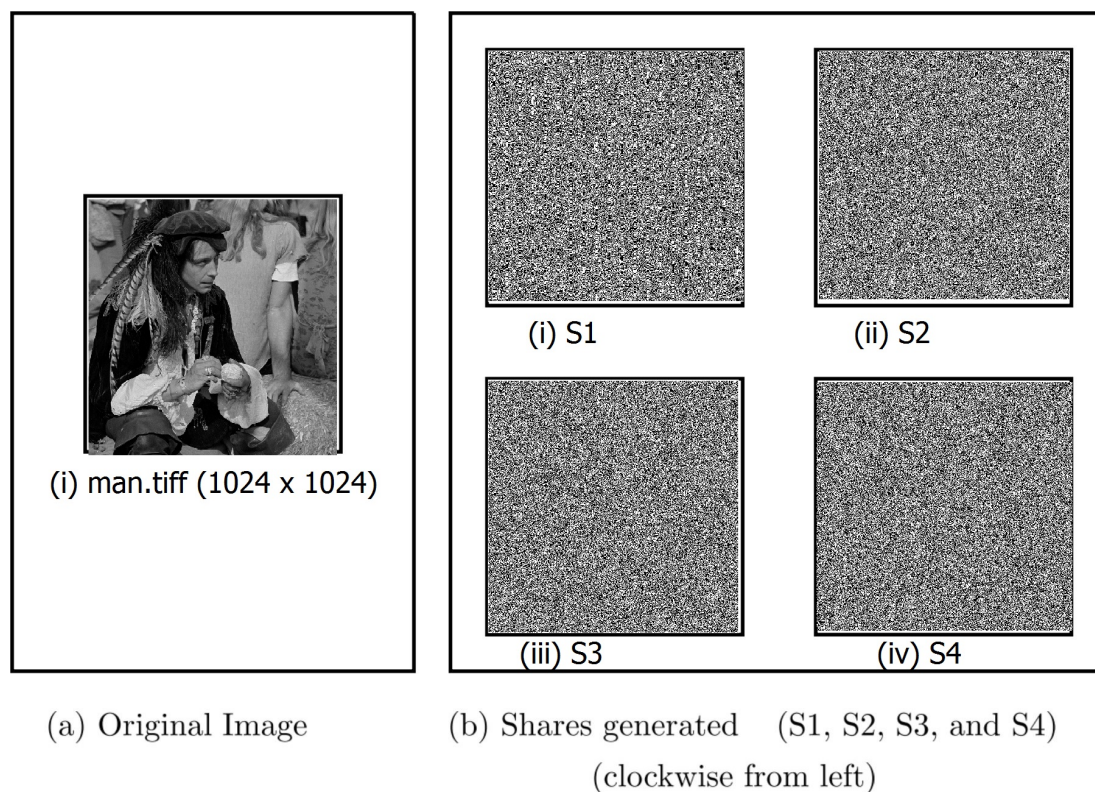


Figure 3.2: Sample shares generated using BPVSS scheme for a man.tiff image. (a) The original image man.tiff of size 1024 x 1024, (b) The four shares generated for the original image S1, S2, S3 and S4

3.1.1 Generation of shares

First step in the proposed scheme is to generate the shares from the original image. The shares are the noise-like images, that alone cannot disclose any information about a SI, hence making the scheme more secure. Shares generation techniques also ensure that information will be revealed in presence of all shares.

The shares can be distributed among n users so that after stacking all n shares participants can recover the SI. The RVSS scheme adapted the technique proposed by [Hou et al. \(2013a\)](#) to generate the noise-like and meaningful shares. The technique proposed by [Hou et al. \(2013a\)](#) has the property that, it progressively recovers the SI by stacking n shares together to reveal SI block by block. It is also called as Block-based Progressive Visual Secret Sharing (BPVSS) scheme. BPVSS scheme generates two types of shares (i) Noise-like and (ii) Meaningful. The noise-like shares are the shares having random salt-pepper noise on cover of shares. The meaningful shares have some meaningful

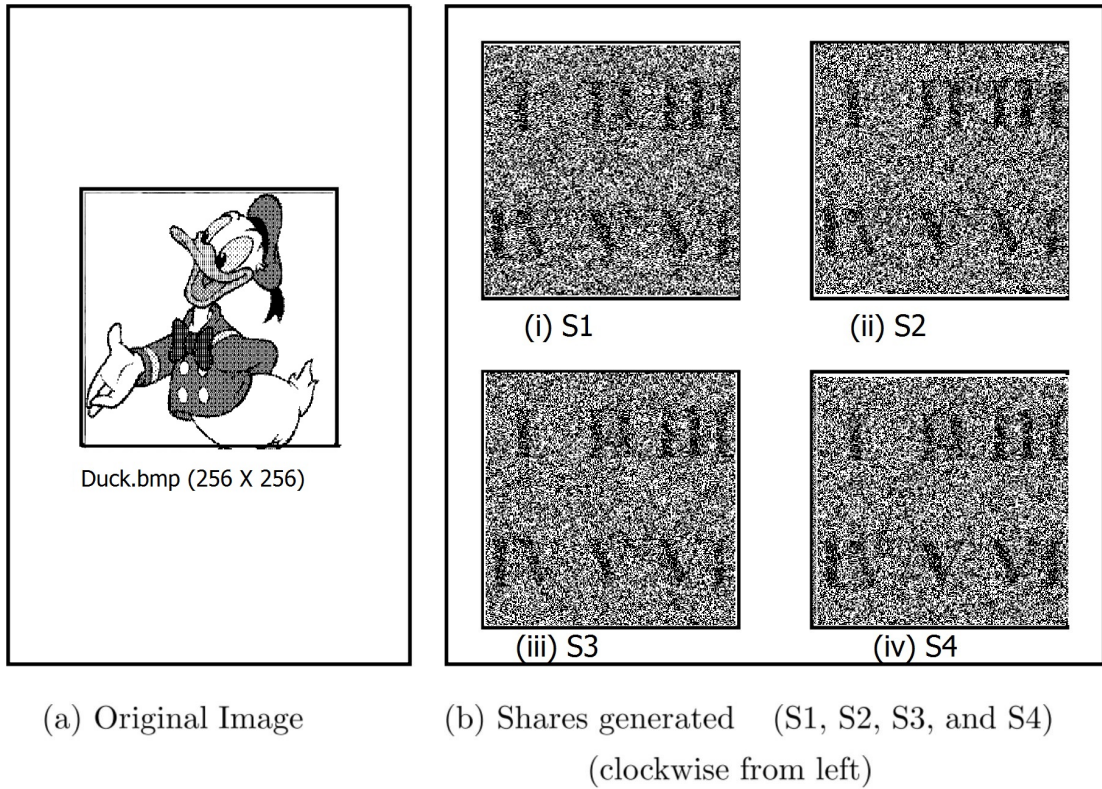


Figure 3.3: Meaningful cover generated for (a) Original image, (b) Shares generated S1, S2, S3, and S4 having another image as cover

cover image imposed on generated shares. Figure 3.2 shows the generated noise-like shares using BPVSS scheme. Figure 3.2 (a) shows the original image and Figure 3.2 (b) shows the generated noise-like shares S1, S2, S3 and S4 respectively. Figure 3.3 shows the meaningful shares with other image used as a cover image. The use of meaningful shares makes transmission of shares less suspicious to intruders. Figure 3.3 (a) shows the original SI and Figure 3.3 (b) shows the four meaningful shares generated for the original SI. The proposed work generates both noise-like and meaningful shares respectively.

Algorithm 3.1 shows the procedure used to generate the content of n shares. The input to the Algorithm 3.1 is secret image converted into a halftone image $I_{halftone}$. The halftone is the commonly used technique by printing media (Wang et al. 2009; Zhou et al. 2006b). The halftone image is a collection of pixels having zeros and ones, it will consider the density of ones and zeros to be used so that image will appear visually similar to gray-scale image. Popular halftone technique using error diffusion

3. Randomized Visual Secret Sharing (RVSS) Scheme

Algorithm 3.1: Generation of shares using BPVSS scheme

Input: 1. The halftone image $I_{halftone}$ having size $W \times H$.
 2. Number of participants n
 3. The $n + 1$ basis matrices such that M^0, M^1, \dots, M^n

Output: The n shares : $S_i, i = 1, 2, \dots, n$ having size $W \times H$

```

1 for row ← 1 to W do
2   for column ← 1 to H do
3     Choose randomly number 1 or 2 and assign it to  $r$ 
4     for  $i \leftarrow 1$  to  $n$  do
5       Let  $Location(row, column) \in Block_m$  where Block follows one of
         the patterns as shown in Figure 3.4.
        1: if  $I_{halftone}(row, column)$  is WHITE then
        2:  $S_i(row, column) \leftarrow M^0(r, i)$ 
        3: else
        4:  $S_i(row, column) \leftarrow M^m(r, i)$ 
        5: end if
6     end
7   end for
8 end
9 end for
10 end
  
```

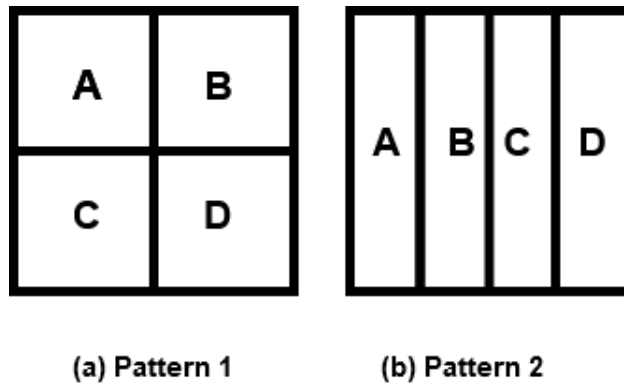


Figure 3.4: Block patterns used by proposed system. (a) The pattern 1 having 4 blocks, (b) The pattern 2 having 4 blocks.

method (Wang et al. 2009) is used in RVSS scheme to convert original image into halftone image. The algorithm also takes number of participants n for which shares needs to be generated as input along with $n + 1$ basis matrices. In the BPVSS scheme, Algorithm 3.1 first logically divide the entire image I having size $W \times H$ into n non-overlapping blocks I_1, I_2, \dots and I_n each of size $\frac{W \times H}{n}$. The sample of non-overlapping blocks are shown in Figure 3.4. For rest of the thesis, same block pattern 1 as shown in Figure 3.4 (a) is used for four participant. The non-overlapping block satisfies the definition given in Equation 3.1

$$\begin{cases} I = \cup I_i & \text{for } 1 \leq i \leq n \\ I_i \cap I_j = \phi & \text{for } 1 \leq i \neq j \leq n \end{cases} \quad (3.1)$$

Equation 3.1 states that original image I can be recovered by stacking all I_1, I_2, \dots, I_n shares. Since BPVSS scheme logically divides the SI into n non-overlapping blocks, recovery of SI follows the pattern like a jig-saw puzzle at the receiver end. Let m represent the block number of the secret image such as $m = 1, 2, \dots, n$ for which shares need to be generated by proposed system. In order to generate n shares, one need to design total $n + 1$ basis matrices such that, M^0 is used for white pixel and M^m for black pixel. Basis matrices are the matrices having value 0 and 1, that is used to process original pixel of SI while generating the shares.

$$M^0 = [\theta_{ij}]_{2 \times n} = \begin{cases} 0, & \text{if } i = 1, 1 \leq j \leq n \\ 1, & \text{if } i = 2, 1 \leq j \leq n \end{cases} \quad (3.2)$$

$$M^m = [\theta_{ij}]_{2 \times n} \begin{cases} 1, & \text{if } i = 1, 1 \leq j = m \leq n \\ 1, & \text{if } i = 2, 1 \leq j \neq m \leq n \\ & \text{where } m = 1, 2, \dots, n \\ 0, & \text{otherwise} \end{cases} \quad (3.3)$$

The matrix M^0 is a collection of two rows having the dimension equal to the total number of users taking part in the sharing process. Equation 3.2 represents the design of basis matrix M^0 for n participants. M^0 is having all elements of the first row initialized to zero and second to ones. Whenever their is a need to process white pixel of SI, refer to M^0 matrix. Now randomly select a row from matrix M^0 to transform white pixel

Table 3.1: Generated basis matrices for $n = 4$

$M^0 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	$M^1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$
$M^2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}$	$M^3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$
$M^4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$	

into n share pixel. Since selection of row is random, matrix M^0 has equal possibility of selecting either row one or row two, hence making the scheme more secure. Also, it makes difficult to guess the generated pixel value in shares. For the black pixel to have the block based reconstruction of an image, design the total n matrices having the same size of $2 \times n$. Equation 3.3 shows n basis matrices generated for a black pixel. The first row of the matrix for $m = 1, 2, \dots, n$ is zero except for the m^{th} block pixel where entry will be one. The Second row in a matrix will be one except pixel having m^{th} block will be zero. To generate n basis matrices for black pixel toggle the pixel at respective block position. Table 3.1 shows the basis matrices generated for block size of 4 (i.e. $m = \{1, 2, 3, 4\}$). Table 3.1 contain total five matrices. M^0 basis matrix is generated with size 2×4 which can be used for processing white pixel. The size of all matrices shown in Table 3.1 are 2×4 , as here for this example the number of participants are four (i.e. $n = 4$). The basis matrices M^1 to M^4 are to be used for processing the black pixel. It can be observed from Table 3.1 that matrices M^1 to M^4 are similar except m^{th} bit, which is toggled for respective matrices.

Let us consider share generation for four participants. To generate the content of shares make use of above generated basis matrices. The basis matrices shown in Table 3.1 provided as input to algorithm along with a number of users as four. Now for each pixel which belongs to $I_{halftone}$ follow Algorithm 3.1. Here this example considers block pattern 1 as shown in Figure 3.4 (a). Let us consider a white pixel at location (x, y) from $I_{halftone}$, that belongs to block A. Since the pixel belongs to block A and

also it is a white pixel, select row one or two (selection of row is random) from basis matrix M^0 and assign them to shares S_1, S_2, S_3 and S_4 respectively at same pixel location of (x, y) in shares. After assignment of values, S_1 will contain value from column one and S_2 to S_4 from respective columns. If selected row is first for basis matrix M^0 , then share S_1 will have pixel 0 assigned to it. Similarly shares S_2, S_3 and S_4 will contain pixel values from respective column i.e. zero for this example. If input image has black pixel, then select basis matrix as M^1 as the pixel belongs to first block pattern (Figure 3.4(a)). Then say randomly selected row of basis matrix M^1 is first row. After this the share S_1 will have pixel value as one assigned to it, and rest of the shares S_2 to S_4 will have pixel values as zero assigned to them. Once all the pixels of $I_{halftone}$ are processed Algorithm 3.1 outputs four shares S_1 to S_4 . Algorithm 3.1 will generate total n shares having size $W \times H$ same as input image. The algorithm can have minimum two and maximum n participants for which shares can be generated, where n should be less than or equal to $W \times H$ (i.e. the size of an input image).

3.1.2 Embedding of data into shares

Step 1 of the RVSS system generates the shares using BPVSS scheme as discussed above (subsection 3.1.1). Once shares are generated make use of Discrete Cosine Transformation (DCT) to transform share into frequency domain. Use middle frequencies to embed data into share as used by Chang et al. (2007); Gujjunoori and Amberker (2013b). This scheme makes use of concept that, Human Visual System (HVS) is less sensitive to changes made in middle frequencies. Gujjunoori and Amberker (2013b) proposed reversible data hiding technique based on the ceaseless zeros to embed pixels into videos. The RVSS system adapts technique proposed by Gujjunoori and Amberker (2013b) to embed the pixel values into shares. The RVSS scheme modified the technique proposed by Gujjunoori and Amberker (2013b) for gray-scale and color images.

Algorithm 3.2 shows the steps performed to embed the data into shares. The RVSS scheme has modified the algorithm proposed by Gujjunoori and Amberker (2013b) to work with images. The RVSS scheme embedded additional information about pixel into shares. Further these pixel values can be used to predict the approximate pixel

Algorithm 3.2: Embedding of data into shares

Input: All n shares as S_1, S_2, \dots, S_n
and original image I having size $W \times H$.

Output: Generates n shares of same size ($W \times H$) with embedded data.

- 1 Partition all shares into block of size 8×8 as $S_i = B_1^i, B_2^i, \dots, B_l^i$ where $1 \leq i \leq n$
- 2 **for** Each $B_j^i \in S_i$ where $1 \leq j \leq l$ **do**
- 3 Calculate the DCT of each B_j^i and then Quantize the DCT coefficients.
- 4 Let $B_k (1 \leq k \leq 9)$ be the set of quantized coefficients of 8×8 each.
- 5 Let z_k be the number of continuous zeros from high frequency to low frequency in set B_k
- 6 **if** ($z_k \geq ((K(k)/2) - 1)$) **then**
- 7 Find the minimum (*min*) and maximum (*max*) value for each set D^k as defined in Figure 3.5 from image I
- 8 Find the middle element position for set D^k as defined in Figure 3.5
- 9 $x = D^k(k, \lceil \frac{K(k)}{2} \rceil)$
- 10 Resolve the Ambiguous condition using
- 11 $A \leftarrow Amb(x)$
- 12 Embed the value at location $D^k(k, \lceil \frac{K(k)}{2} \rceil)$ using
- 13 $E \leftarrow Embed(A, (min/max))$
- 14 // *min* is embedded in even shares and *max* in odd shares.
- 15 **end if**
- 16 **end**
- 17 **end for**
- 18 **end**

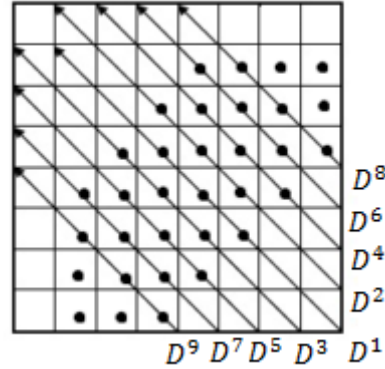


Figure 3.5: Nine sets defined for data embedding

values at the receiver end.

Consider n shares S_1, S_2, \dots, S_n generated in the previous step for reversible hiding of data. Algorithm 3.2 shows the various steps performed to embed the data into shares. Algorithm 3.2 takes secret image I having size $W \times H$ as input along with shares. In order to embed data into shares first, partition each shares S_i into multiple blocks $B_1^i, B_2^i, \dots, B_l^i$ of size 8×8 . The B_j^i represents j^{th} block of the i^{th} shares. For each block compute the DCT coefficient using Equation 3.4. The $F_{u,v}$ represents the coefficient at the coordinate (u, v) in the frequency domain. It computes the coefficient value at u, v location for the 8×8 block. $B_l^i(s, t)$ is the location of pixel value for i^{th} share in the spatial domain and $l = \{1, 2, \dots, (W \times H)/64\}$. To hide the data into shares, first transform the shares into frequency domain using DCT, that will generate coefficient from low to high frequency for given block of share.

$$F_{u,v} = \frac{C(u) \times C(v)}{4} \sum_{s=0}^7 \sum_{t=0}^7 B_l^i(s, t) \times \bar{f}(s, t, u, v) \quad (3.4)$$

where $0 \leq u, v \leq 7$ and

$$\bar{f}(s, t, u, v) = \cos \frac{(2s+1)u\pi}{16} \cos \frac{(2t+1)v\pi}{16},$$

$$C(e) = \begin{cases} \frac{1}{\sqrt{2}} & e = 0 \\ 1 & e > 0 \end{cases}.$$

The high frequency coefficient needs to be quantize to zero for better embedding capacity. To achieve this RVSS scheme uses standard quantization table as shown in

Table 3.2: The standard quantization table

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Table 3.2. For rest of thesis chapters same quantization table as shown in Table 3.2 will be used. After quantization high frequency coefficient will be reduced to zero, which will provide more hiding capacity.

The HVS is less sensitive to changes made in the middle frequencies. Embedding data in middle frequency will maintain shares visually similar. To achieve the middle frequency embedding, quantize the coefficient using standard quantization table. To embed the data into shares define the sets as D^1, D^2, \dots, D^9 . Figure 3.5 shows the sets D^k ($1 \leq k \leq 9$) used by the RVSS system to hide pixel data. For the rest of thesis chapters same nine set locations will be used to embed data as shown in the Figure 3.5.

Now select a middle position of each set as a desire location for hiding pixel data. Make use of ceaseless zero frequency locations to embed data. Count the ceaseless zero z_k in the given set D^k from low to high frequency. If z_k value is greater than or equal to $\lceil \frac{K(k)}{2} \rceil - 1$ for k^{th} set as defined in Figure 3.5 then choose middle element as location for embedding data. Once the location of embedding is found out select the minimum and maximum value of the pixel for each set of block from secret image I having size $W \times H$. Embed the values at that position such that even shares contain the minimum values and odd shares contain maximum values. Let s be the minimum or maximum value for given set and $x = D^i(i, \lceil \frac{K(k)}{2} \rceil)$ be the coefficient value at middle location in given set.

Now to embed the pixel value s , sender must take care of ambiguous condition.

Table 3.3: Size of each chosen sets for embedding. k is the set number and $K(k)$ indicates the size of the respective set

k	1	2	3	4	5	6	7	8	9
K(k)	7	7	7	6	6	5	5	4	4

Ambiguous condition arises when receiver try to extract the data at extraction side, but they are not sure about the data (pixel s), whether it is embedded or not. Let us consider the set D^1 having sequence of coefficient from low to high as $(0, 0, 0, 2, 1, 6, -2)$. According to Table 3.3 for set D^1 ceaseless zero should be 3 (i.e. $\lceil \frac{7}{2} \rceil - 1$), now select middle position to embed the pixel value. For rest of the thesis chapters make use of same Table 3.3 to choose the size of the sets required to embed pixel values. Let us consider pixel value present at the middle location is 2 and if sender is also embedding minimum value of pixel as 2 then receiver might make a false judgment, while extracting data from set D^1 . The receiver might consider DCT coefficient value as a hidden pixel value. To solve the ambiguity as well as ensuring the restoration of coefficient, modify the coefficient using Amb function defined in Equation 3.5. When value of x is zero embed the data so function will return zero. As this scheme tries to embed minimum and maximum value of pixel, which will have values from 0 to 255. Considering the nature of pixel values proposed scheme adds 256 to x for positive coefficient and subtract 256 from negative coefficient. It helps in resolving ambiguous condition of data being embedded at that location. Once ambiguous condition is resolved, make use of $Embed$ function defined in Equation 3.6 to decide which values to embed at given location. Let s be the value which sender wish to embed into shares. It can be either minimum or maximum pixel value. If the position value is zero then embed s , else embed modified value at that location. So for the above given sequence, according to Amb function, the value for A will be 258. It indicates that the location chosen for embedding is ambiguous, which will be used to restore the shares back to original state and extract any information hidden into share. Restoration and extraction will be discussed

in Section 3.1.3

$$A = Amb(x) = \begin{cases} 0 & \text{if } x = 0 \\ x + 256 & \text{if } x \geq 1 \\ x - 256 & \text{Otherwise,} \end{cases} \quad (3.5)$$

$$E = Embed(A, s) = \begin{cases} s & \text{if } A = 0 \\ A & \text{Otherwise,} \end{cases} \quad (3.6)$$

Once the values are embedded, send these shares to the participants. The reason behind embedding minimum and maximum value is that, if sender embed the real pixel values into the shares, then each share can reveal some information related to the secret image which will make the scheme vulnerable. Hence this scheme is embedding only minimum and maximum values and not embedding actual value into scheme to make it secure. This scheme is adding random pixel information based on actual minimum and maximum values for each block into the sets that are defined in Figure 3.5.

3.1.3 Extraction of data and reconstruction of image

Once data is embedded into shares, transfer these shares over the network to participants. Receiver extracts the hidden information from each pattern, that is used for embedding data. Extraction of data is the inverse procedure of embedding. Algorithm 3.3 shows the extraction of data at receiver end. Input to the Algorithm 3.3 is all the shares S_1, S_2, \dots, S_n of size $W \times H$. Algorithm 3.3 restores the original shares and also returns matrices containing hidden data. To extract data from shares, partition all shares into block of size 8×8 as $S_i = B_1^i, B_2^i, \dots, B_l^i$. B_l^i represent l^{th} block of i^{th} shares and $i = 1, 2, \dots, n$. Then for each block of shares find the location of embedded data based on count of ceaseless zero. To find the location receiver counts the ceaseless zero for each set defined in Table 3.3. Let z_k be the count of ceaseless zeros for k^{th} set. Let z_k is greater than or equal to $\lceil \frac{K(k)}{2} \rceil - 1$ then consider middle frequency coefficient as desire location. Once location of embedding is found use *ExtractData* function as shown in Equation 3.7 to extract the data embedded at that location and *Restore* as shown in Equation 3.8 to restore back original coefficient. The extraction algorithm is same

Algorithm 3.3: Extraction of data from shares and restoration of shares	
Input:	All n shares as S_1, S_2, \dots, S_n having size $W \times H$.
Output:	The n shares S_i with restored values and n marices containing Extracted Data E_i , where $i = 1, 2, \dots, n$
1	Partition all shares into block of size 8×8 as $S_i = B_1^i, B_2^i, \dots, B_l^i$ where $1 \leq i \leq n$;
2	for Each $B_j^i \in S_i$ where $1 \leq j \leq l$ do
3	Let $B_k (1 \leq k \leq 9)$ be the set of quantized coefficients of 8×8 each.
4	Let z_k be the number of continuous zeros from high frequency to low frequency in set B_k
5	if ($z_k \geq ((K(k)/2) - 1)$) then
6	Find the middle element position for set defined in Figure 3.5
7	$x = D^k(k, \lceil \frac{K(k)}{2} \rceil)$
8	Extract the information about embedded data using Equation 3.7
9	$E_i^j \leftarrow ExtractData(x)$
10	Restore the initial value at middle location using Equation 3.8.
11	$B_i^j \leftarrow Restore(x)$
12	end if
13	end
14	end for
15	end
16	Combine all the B_j^i such that $S_i = \{B_1^i, B_2^i, \dots, B_l^i\}$;
17	Combine all the E_j^i such that $E_i = \{E_1^i, E_2^i, \dots, E_l^i\}$;

as that of embedding except it will use *Restore* and *ExtractData* function instead of *Embed* at receiver end. Let x be the coefficient value available at the middle location in a set D^i . The function *ExtractData* will return value as embedded value if it lies in the range from 0 to 255 otherwise it means receiver had not embedded any data at that location. The value $D = 0$ represents no data is embedded. The function *Restore* restores the original coefficient value based on conditions given in Equation 3.8. Now de-quantize the shares by multiplying with same quantization table as shown in Table 3.2 used for embedding of data. Apply Inverse Discrete Cosine Transform (IDCT) to restore back the original pixel value of shares. Combine all blocks into respective shares to get shares having initial pixel values before embedding of data.

$$D = \text{ExtractData}(x) = \begin{cases} x & \text{if } 0 \leq x \leq 255 \\ 0 & \text{Otherwise,} \end{cases} \quad (3.7)$$

$$D = \text{Restore}(x) = \begin{cases} 0 & \text{if } 0 \leq x \leq 255, \\ x - 256 & \text{if } x \geq 256, \\ x + 256 & \text{Otherwise,} \end{cases} \quad (3.8)$$

Algorithm 3.3 output matrices E_i , which contains the minimum and maximum values. For each even matrix E_i where i is even extract the unique entries corresponding to same location in all shares and store it in E_{max} . Similarly, for odd matrices extract unique pixel value and store it in E_{min} . Once the minimum and the maximum values are extracted from the embedded shares at the receiver end, make use of these values to generate the matrix E_{final} using E_{min} and E_{max} . Embed the random values within a range from minimum to maximum at middle and its neighbor location as shown in Figure 3.5.

By extracting the embedded information, the secret shares are restored to their original value using Algorithm 3.3. All the users can stack the shares together to recover the secret image. To stack shares together receiver uses simple OR operation. The reconstructed image is the result of BPVSS scheme as shown in Figure 3.7. Note that reconstructed image is having only ones and zeros as pixel values.

3.1.4 Embedding data back into image

Secret image is recovered using simple OR operation in the above step. The above step also (subsection 3.1.3) extracted the minimum/maximum pixel value information embedded by the sender into shares. But, original image has the values in the range 0 to 255. Now apply inverse halftone technique on the recovered SI to get estimated values for SI. There are many techniques proposed by researchers to get inverse halftone image like Chung and Wu (2005); Kite et al. (2000); Mese and Vaidyanathan (2001); Xiong (1999). The RVSS scheme uses wavelet-based inverse halftone technique proposed by Xiong (1999). Inverse halftone is the process of estimating the values of pixel from the halftone image. Once estimated image is obtained using inverse half-toning, receiver embeds data back into image to proliferate visual quality. Now embed data matrices E_{final} obtained using Algorithm 3.3 containing the random values (33 out of 64 for each block of size 8×8). E_{Final} contain information about original image I which can be used to improve contrast of image. Replace those values in inverse halftone image at respective locations. After embedding of data into reconstructed image, it still contain the random noise which is generated while creating shares. The noise itself affects the contrast of image, which reduces the quality of image. In order to mitigate the effect of random noise post processing is done. Wiener filter is used to filter the noise. This boosts the contrast of final image by reducing the noise from image. The Wiener filter works based on estimating statistical parameter like mean and variance using pixel wise adaptive Wiener method. With the help of embedded information about original image RVSS scheme is able to improve the quality of final image.

3.2 EXPERIMENTAL RESULTS

The experiments were conducted on system having Intel i7-4790 processor with 16 GB RAM, having matlab 2015a as development environment on windows 10 operating system. The RVSS scheme used the image database available at (of Southern California 1977) provided by USC University of southern California (Signal and image processing institute) and from Y. C. Hou's official website (Hou 2012). The dataset contains total of 44 images, 16 color, 28 gray-scale and 2 binary images. The sizes of dataset are

256 × 256 (14 images), 512 × 512 (26 images) and 1024 × 1024 (4 images).

The RVSS scheme generated two types of shares (i) Noise-like and (ii) shares having meaningful cover (meaningful). The noise-like shares are the shares containing random salt-pepper noise on it. Whereas meaningful shares contains visual image imposed on them that is different from secret image. Figure 3.2 shows the shares generated containing noise-like cover on top of secret image, also Figure 3.3 shows the meaningful shares with other image as cover for shares. The use of meaningful shares makes transmission of shares less suspicious to intruders.

The RVSS scheme takes $O(WH)$ time to generate shares as it has to process each pixel, where W is the width of an image and H is the height of an image. To embed data it also takes $O(WH)$ time. Therefore overall time complexity at sender end is $O(WH)$. At the receiver end major time complexities involved are extraction of data which is of the order $O(WH)$ and inverse halftone operation having $O(WH)$ complexity. The stacking operation and embedding of extracted data into shares takes constant time of $O(1)$. The overall time complexity of the algorithm is $O(WH)$ at receiver end too.

Popular metrics for evaluating the similarity between the original and restored image are being used for this scheme. To evaluate the reconstruction quality of an image, experimental results with various image quality parameters like mean square error (MSE), peak signal-to-noise ratio (PSNR), Normalized cross correlation (NCC), and Normalized absolute error (NAE) had been carried out in this chapter.

3.2.1 Mean Square Error -HVS (MSE^{HVS})

It is the measurement of quality of recovered image to the original image. It computes a positive value from 0 to 1, values near to 0 represent better visual quality of image. The mean square error is computed using Equation 3.9. It computes the square of difference between original image I and recovered image R . In the Equation 3.9 m and n is the size of image. Proposed scheme compared MSE^{HVS} with the BPVSS scheme which recovers image using block based stacking of image. Table 3.4 shows the comparison with BPVSS for both noise-like and meaningful shares. From Table 3.4 it is evident that proposed method gives value of MSE near to zero as compared to BPVSS scheme.

Table 3.4: Mean square error-HVS value for various test images

Test Image	Size	Type	RVSS		BPVSS	
			Noise-like	Meaningful	Noise-like	Meaningful
Girl	256	color	0.031	0.032	0.3945	0.4706
Couple	256	color	0.018	0.016	0.4511	0.5328
House	256	color	0.054	0.093	0.4987	0.5642
Tree	256	color	0.05	0.107	0.1556	0.2456
Airplane	256	gray-scale	0.048	0.071	0.4217	0.6107
Clock	256	gray-scale	0.051	0.026	0.2451	0.5645
Couple	512	gray-scale	0.023	0.11	0.4634	0.6577
Man	1024	gray-scale	0.017	0.035	0.3201	0.6512

For test image "clock" BPVSS computes MSE as 0.2451 whereas RVSS scheme gives value as 0.051 for noise-like shares. As stated above it is near to zero means recovered image is better as compared to BPVSS scheme.

$$MSE^{HVS} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - R(i, j)]^2 \quad (3.9)$$

3.2.2 Peak Signal-to-Noise Ratio (PSNR)

PSNR is the ratio between the maximum possible power of signal to the corrupting noise added in original signal. It mainly provides an approximation to human visual system. Higher the value of PSNR, better is the visual quality. The formula used to compute PSNR is shown in Equation 3.10. PSNR is computed by taking logarithmic ratio of maximum value in image to the MSE for images to base 10. PSNR is usually measured in logarithmic decibel scale (dB). Images having the higher decibel value are the images having better visual quality. For the image "clock" BPVSS has PSNR of 54.2374 dB for noise-like shares whereas proposed method gives better PSNR value as 61.088 dB, which gives better visual quality. Table 3.5 shows the PSNR values for gray-scale and color images for both noise-like and meaningful shares.

$$PSNR = 10 \cdot \log_{10} \frac{255^2}{MSE^{HVS}}, (dB) \quad (3.10)$$

3. Randomized Visual Secret Sharing (RVSS) Scheme

Table 3.5: Peak signal-to-noise ratio (PSNR) value for various test images (in dB)

Test Image	Size	Type	RVSS		BPVSS	
			Noise-like	Meaningful	Noise-like	Meaningful
Girl	256	color	63.185	63.02	54.9823	48.3780
Couple	256	color	65.692	65.958	54.3289	47.8261
House	256	color	60.786	58.45	55.3641	47.1272
Tree	256	color	61.15	57.828	56.2114	49.6327
Airplane	256	gray-scale	61.339	59.623	54.0019	46.8364
Clock	256	gray-scale	61.088	64.062	54.2374	50.6142
Couple	512	gray-scale	64.44	57.717	55.3217	51.7624
Man	1024	gray-scale	65.755	92.694	55.3654	49.4328

3.2.3 Normalized Cross Correlation (NCC)

NCC evaluates the quality of distorted image with respect to original image. Normalized Cross Correlation (NCC) lies between 0 and 1 in which 1 stand for symmetric images and 0 for nonidentical images. The formula used for computing NCC is given in Equation [3.11](#).

$$NCC = \sum_{i=1}^X \sum_{j=1}^Y \frac{I_{i,j} \cdot R_{i,j}}{I_{i,j}^2} \quad (3.11)$$

Table [3.6](#) shows the values for various test images. For “clock” BPVSS gives NCC as 0.5001 whereas proposed method provides NCC as 0.815, which also means proposed method has 81.5% contrast as compared to BPVSS having 50% contrast. For all other images proposed method gives contrast from 70% to 90% as compared to BPVSS scheme having 49% to 50% contrast. Contrast is the difference of color and illumination, which makes object visible or perceptible. In visual perception contrast is computed as difference between color and brightness with respect to same field of view for different objects. The RVSS method tries to recover the original pixel value by embedding data and also removing noise after applying inverse halftoning into shares recovered image. As various parameter suggest proposed method provides better visual quality having almost 70-90% contrast for noise-like shares. For meaningful shares BPVSS provides 25% contrast whereas proposed method provides better contrast of

Table 3.6: Normalized Cross Correlation (NCC) value for various test images

Test Image	Size	Type	RVSS		BPVSS	
			Noise-like	Meaningful	Noise-like	Meaningful
Girl	256	color	0.777	0.718	0.4998	0.2489
Couple	256	color	0.703	0.701	0.4879	0.2484
House	256	color	0.798	0.641	0.5010	0.2479
Tree	256	color	0.853	0.671	0.4435	0.2364
Airplane	256	gray-scale	0.64	0.526	0.5002	0.2498
Clock	256	gray-scale	0.815	0.574	0.5001	0.2483
Couple	512	gray-scale	0.792	0.73	0.4987	0.2503
Man	1024	gray-scale	0.906	0.807	0.5003	0.2481

70-80% for recovered image.

3.2.4 Normalized Absolute Error (NAE)

Normalized Absolute Error (NAE) is computed using Equation 3.12, where I is the original image and R is the recovered image. It is the ratio of difference between the pixel to the original image pixel (i.e. error to the original image pixel). It will compute the error present in recovered image, if value of NAE is close to 0 means image has better quality. The image with larger value is said to have poor quality. Table 3.7 shows the values for test images, BPVSS has value of 0.5001 for “clock” whereas proposed method has NAE value as 0.259 for the noise-like shares. It is evident from the Table 3.7 that proposed RVSS has shown significant decrease in the error values for the images from 0.7153-0.7510 to 0.124-0.616 for the meaningful images. The decrease in the reconstruction error is achieved due to use of embedded pixel values.

$$NAE = \sum_{i=1}^X \sum_{j=1}^Y \frac{I_{i,j} - R_{i,j}}{I_{i,j}} \quad (3.12)$$

Figure 3.6 shows sample color images used for experiment. All color images shown in Figure 3.6 (a-d) are having size of 256×256 . Similarly Figure 3.9 shows the gray-scale images used for experiment. Figure 3.9 (a-b) has image size of 256×256 , Figure 3.9 (c) has size of 512×512 and Figure 3.9 (d) has image size of 1024×1024 . The Figure 3.7 and Figure 3.10 show the recovered color and gray-scale images using the

3. Randomized Visual Secret Sharing (RVSS) Scheme

Table 3.7: Normalized Absolute Error (NAE) value for various test images

Test Image	Size	Type	RVSS		BPVSS	
			Noise-like	Meaningful	Noise-like	Meaningful
Girl	256	color	0.65	0.616	0.5010	0.7502
Couple	256	color	0.245	0.263	0.4989	0.7492
House	256	color	0.372	0.431	0.5001	0.7498
Tree	256	color	0.364	0.494	0.5002	0.7153
Airplane	256	gray-scale	0.252	0.399	0.5002	0.7510
Clock	256	gray-scale	0.259	0.155	0.5001	0.7487
Couple	512	gray-scale	0.255	0.124	0.4967	0.7485
Man	1024	gray-scale	0.262	0.38	0.4998	0.7498

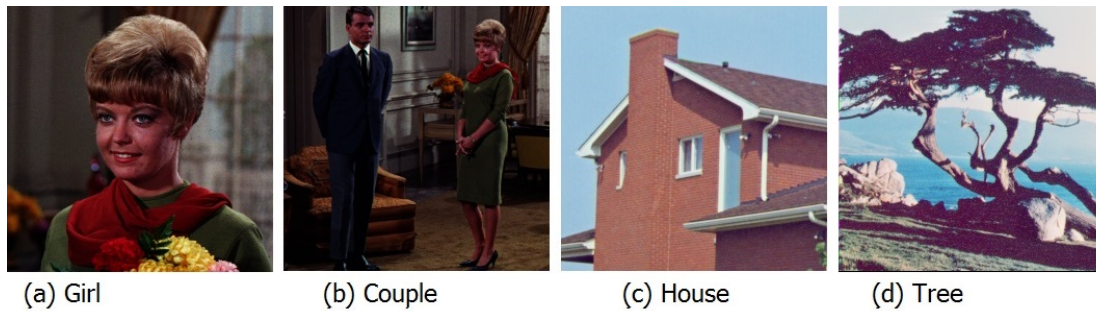


Figure 3.6: The sample original color images used for the experiment as (a) Girl, (b) Couple, (c) House, and (d) Tree

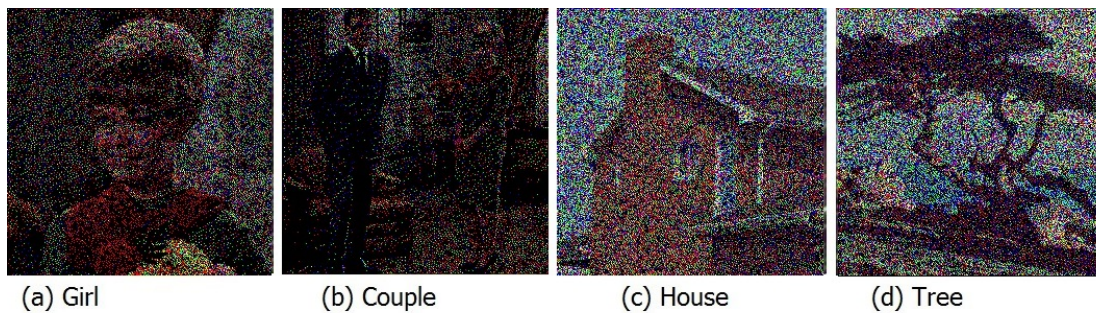


Figure 3.7: Output of BPVSS (Hou et al. 2013a) scheme for color images. (a) Girl, (b) Couple, (c) House, and (d) Tree

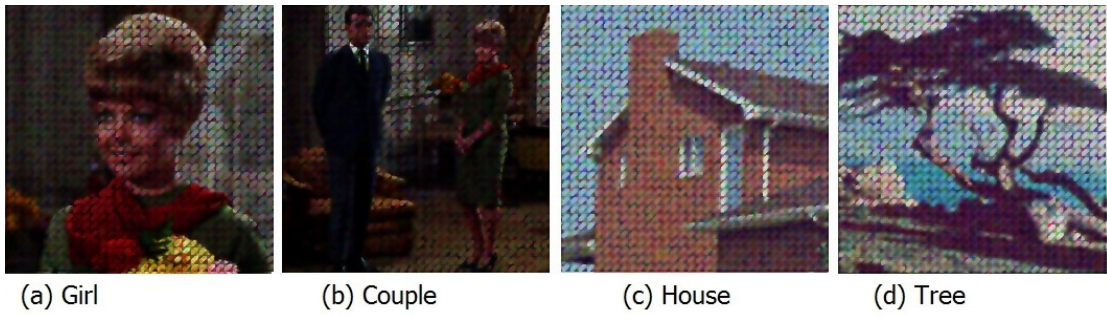


Figure 3.8: Output of RVSS (Mhala et al. 2018) scheme for color images. (a) Girl, (b) Couple, (c) House, and (d) Tree

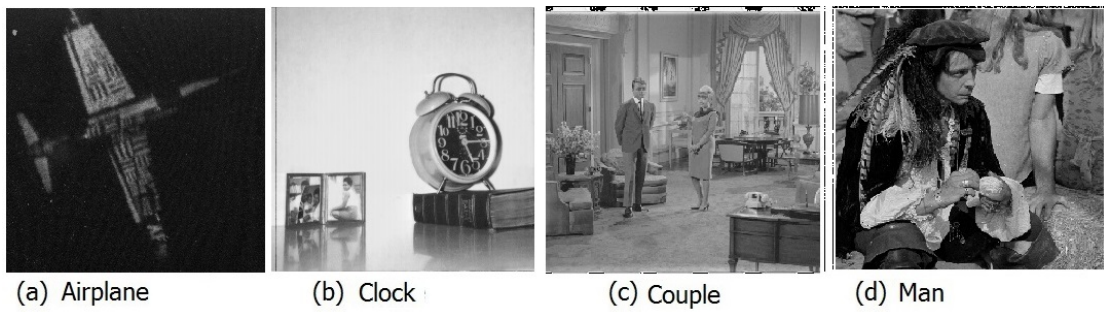


Figure 3.9: Gray-scale images used for experiment as (a) Airplane, (b) Clock, (c) Couple, (d) Man

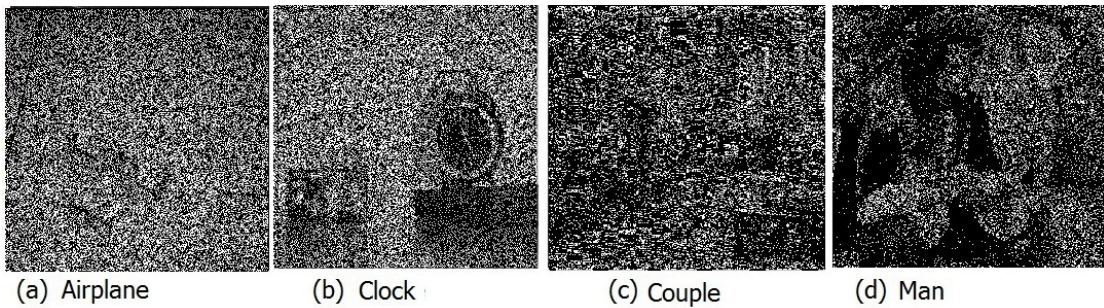


Figure 3.10: Output of BPVSS (Hou et al. 2013a) scheme for gray-scale images a) Airplane, (b) Clock, (c) Couple, (d) Man

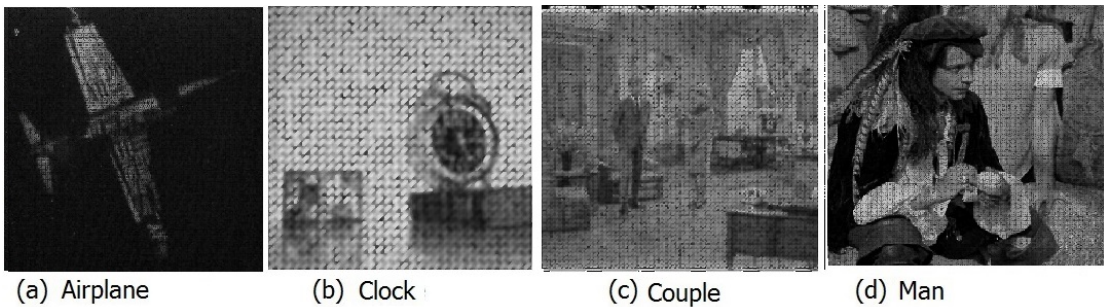


Figure 3.11: Output of RVSS (Mhala et al. 2018) scheme for gray-scale images a) Airplane, (b) Clock, (c) Couple, (d) Man

BPVSS scheme. Poor contrast of BPVSS images is visually evident from Figure 3.6 and Figure 3.9. Whereas from Figure 3.8 and Figure 3.11 improved contrast of images can be observed. The images recovered using RVSS scheme have almost 75-80 % contrast, which better than BPVSS scheme (25-50% contrast).

3.3 SUMMARY

This chapter presented a VSS technique called Randomized Visual Secret Sharing (RVSS) scheme for gray-scale and color images. The RVSS scheme uses Block-based VSS scheme to generate the shares. Once shares are generated, then scheme embeds the pixel information into shares. The embedded pixel information works as a cue to improve the contrast and visual quality of the reconstructed image.

The technique presented in this chapter provides the solution to poor contrast problem of block-based VSS scheme. the scheme proposed in this chapter recovers SI with a better contrast of 70-90% for gray-scale and color images as compared to BPVSS scheme having a maximum contrast of 50%. Also, the technique presented in this chapter reconstructs the secret image in the multi-tone format as compared to BPVSS scheme (i.e. binary image).

CHAPTER 4

CONTRAST ENHANCEMENT OF RANDOM VISUAL SECRET SHARING SCHEME

Visual Cryptography (VC) is a cryptographic technique which permits visual information (e.g. written notes, picture, and printed text) to be encrypted in such a way that the decryption can be performed by the Human Visual System (HVS). Although many cryptographic algorithms (eg. DES, AES, DSA etc.) exist to secure secret information, they use complex mathematical operations to perform encryption and decryption. Visual Secret Sharing (VSS) is a perfectly secure method first introduced by [Naor and Shamir \(1994a\)](#) to share visual information in the field of VC. VSS schemes transmit the secret image by splitting it into multiple shares (n). The shares are the encrypted version of the secret image, that themselves do not possess any valuable information related to the secret image. To decrypt the secret information, participants need to join at least k (or more) shares together out of n shares. Hence it is also referred as (k,n) threshold scheme. Failing to stack at least k shares out of n will not reveal any visual information about the secret image.

Although Naor and Shamir proposed basic VSS scheme, it suffers from common drawbacks like 1) Generation of shares having increased size, and 2) Noise-like shares generation. The generation of shares with expanded shares leads to more bandwidth utilization. The Noise-like shares are visually identical, so it creates confusion among participants while distributing the shares. The traditional VSS schemes require all the shares to be stacked together in order to recover the secret image. Whereas, Progressive

VSS (PVSS) schemes are the recent development in the field of VSS. PVSS recovers the partial part of secret, which can be visualized by participants. The advantage of PVSS is that part of the secret information will be available to users if they can stack some predefined shares.

Randomized VSS (RVSS) scheme is a PVSS based scheme proposed by [Mhala et al. \(2018\)](#) (Chapter [3](#)). This scheme uses the concept of data embedding into shares to improve the contrast of recovered images. Although scheme recovers the secret image in the multitone format with 70-80% contrast, it still suffers from the poor contrast ([Hou et al. 2013a](#); [Mhala et al. 2018](#)) problem. Since RVSS uses random pixels to improve the contrast of the recovered image, that results in addition of blocking artifact. The main contributions of this chapter are as follows:

- Presented an efficient contrast enhancement scheme for RVSS using multiple image Super-resolution (SR).
- Presented a technique to embed low-resolution data into shares to reduce blocking artifact.

Rest of the chapter is organized as follows. Section [4.1](#) briefs about a novel Super-resolution based Visual Secret Sharing (SRVSS) scheme proposed to improve the contrast of the recovered secret image. The experimental results are presented in Section [4.2](#). Finally, Section [4.3](#) summarizes the chapter.

4.1 A SUPER-RESOLUTION BASED VISUAL SECRET SHARING (SRVSS) SCHEME

Super-resolution is being used in many areas like medical image processing, facial image analysis, etc., to improve the quality of the images. The SRVSS scheme discussed in this chapter adapts the super-resolution based technique to improve contrast of the RVSS scheme. To achieve this goal, proposed scheme embeds additional information about the secret image inside the shares. Section [4.1.2](#) discuss the embedding of data into the shares in detail. Figure [4.1](#) provides an overview of the SRVSS system. The various steps involved in the SRVSS system are explained below.

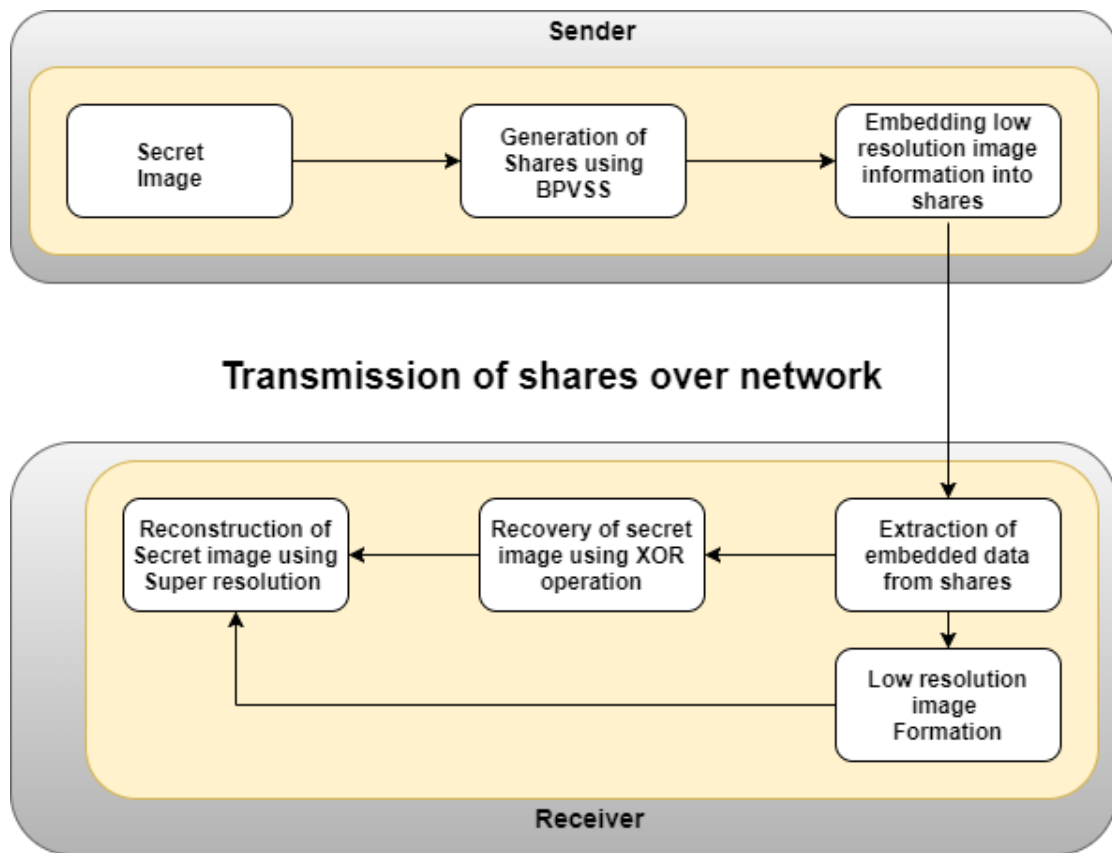


Figure 4.1: The Flowchart of the SRVSS system

4.1.1 Share generation using BPVSS

First step in the SRVSS system is to generate shares for the secret image. This chapter, uses same Block-based Progressive VSS (BPVSS) scheme to generate shares as discussed in Chapter 3. This chapter also generates two types of shares namely meaningful and noise-like shares. The Noise-like shares are the shares which have random noise-like appearance and meaningful shares have any other image (different from the secret image) imposed on the shares. The image used in the meaningful shares acts as cover image giving more visual meaning to shares. Shares generated using BPVSS scheme for the Secret Image (**SI**) satisfies the definition given in Equation 4.1. Here $\mathbf{SI}_1, \mathbf{SI}_2.. \mathbf{SI}_n$ are the shares generated for the secret image **SI**.

$$\begin{cases} \mathbf{SI} = \cup \mathbf{SI}_i & \text{for } 1 \leq i \leq n \\ \mathbf{SI}_i \cap \mathbf{SI}_j = \phi & \text{for } 1 \leq i \neq j \leq n \end{cases} \quad (4.1)$$

Equation 4.1 shows that secret image **SI** can be recovered by stacking all $\mathbf{SI}_1, \mathbf{SI}_2.. \mathbf{SI}_n$ shares. Also each share should be independent in order to transmit shares securely. Let us consider the secret image of *Lenna* as shown in Figure 4.2 (a) as an example, which needs to be shared among four participants ($n=4$). The dimension of the secret image **SI** is 512×512 in this example. Figure 4.3 shows the four shares generated for the secret image *Lenna* using BPVSS scheme.

4.1.1.1 Preliminaries for generating shares

Share generation algorithm mainly takes basis matrices as input for generating shares. The basis matrices are the collection of zeros and ones. These matrices are used to generate shares. The design of basis matrices ensures that it should satisfy the definition given in Equation 4.1. In order to generate n shares one need to form $n + 1$ basis matrices. The basis matrix has the dimension of $2 \times n$. The basis matrix \mathbf{B}^0 is designed for white pixel and $\mathbf{B}^1.. \mathbf{B}^n$ matrices are designed for black pixel. The basis matrix \mathbf{B}^0 contains two rows and n columns. The first row of the \mathbf{B}^0 matrix contains all zeros and second row contains all ones.

$$\mathbf{B}^0 = [\theta_{ij}]_{2 \times n} = \begin{cases} 0, & \text{if } i = 1, 1 \leq j \leq n \\ 1, & \text{if } i = 2, 1 \leq j \leq n \end{cases} \quad (4.2)$$



Figure 4.2: The sample input images used : (a) the secret image (lenna.tiff) (\mathbf{SI}) (b) Halftone image generated from secret image ($\mathbf{SI}_{halftone}$)



Figure 4.3: The shares generated for four participants. (a) Share of participant 1 (\mathbf{SI}_1) (b) Share of participant 2 (\mathbf{SI}_2) (c) Share of participant 3 (\mathbf{SI}_3) and (d) Share of participant 4 (\mathbf{SI}_4)

Table 4.1: Generated basis matrices for $n = 4$

$\mathbf{B}^0 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	$\mathbf{B}^1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$
$\mathbf{B}^2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}$	$\mathbf{B}^3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$
$\mathbf{B}^4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$	

$$\mathbf{B}^m = [\theta_{ij}]_{2 \times n} \begin{cases} 1, & \text{if } i = 1, 1 \leq j = m \leq n \\ 1, & \text{if } i = 2, 1 \leq j \neq m \leq n \\ & \text{where } m = 1, 2, \dots, n \\ 0, & \text{otherwise} \end{cases} \quad (4.3)$$

Equation 4.2 gives the basic matrix generated for white pixel. Equation 4.3 gives the basis matrices designed for the black pixel. For the black pixel we need total n matrices. The basis matrix \mathbf{B}^1 contains first row as zeros and second row as ones except for first column, where values are being toggled (i.e. one becomes zero and vice versa). Similarly for the \mathbf{B}^m basis matrix first row is a collection of zeros and second row is a collection of ones except for m^{th} column. The m^{th} column values are toggled. The share generation algorithm also takes halftone image of a secret image as input. The VSS make use of halftone technique to generate shares for gray-scale and color images. The researchers have proposed many techniques to generate halftone image from gray-scale image. Figure 4.2 (b) shows the halftone image generated for a Secret Image (SI). In this chapter, the SRVSS scheme considered Floyd's Error Diffusion Method (Wang et al. 2009) to generate halftone image. Once secret image gets transformed into halftone format, the pixel information gets lost. In order to recover the actual pixel information the SRVSS scheme will make use of hidden information and SR technique, which will be discussed in section 4.1.2 and 4.1.4 respectively.

4.1.1.2 Share Generation Algorithm

To generate the shares for n participants make use of designed basis matrices defined in Table 4.1. The algorithm for generation of shares using BPVSS scheme is described in Algorithm 4.1. The input to the BPVSS algorithm is a halftone image ($\mathbf{SI}_{\text{halftone}}$). Now label the entire image into multiple blocks m as shown in Figure 3.4. Please note that, the block pattern used in this chapter is same as that is used in Chapter 3. Here m is the block number ranging from one to n ($m = 1, \dots, n$). The part of the pattern is shown in Figure 3.4 works like a piece in zig-saw puzzle. In order to generate n shares select the secret pixel from halftone image. If the secret image pixel is white, then make use of basis matrix \mathbf{B}^0 . Once, basis matrix is selected, now make random selection of row from basis matrix \mathbf{B}^0 and assign new values to respective shares. The share 1 will have value pertaining to column 1 and so on for the rest of shares. If the secret image pixel is black and it belongs to m^{th} block, then choose the basis matrix \mathbf{B}^m . Once basis matrix is selected for black pixel, randomly select the row from chosen basis matrix. Assign the m^{th} column pixel to m^{th} share to generate the shares. The random selection of row from the designed basis matrices, makes scheme more secure. As selection of row is random one cannot predict the values assigned to the shares.

Lets us consider the share generation for four participants ($n = 4$) for a secret image \mathbf{SI} with an example. First step before generating the shares is to design the basis matrices. For this example one need to design total $n + 1$ matrices. The basis matrices $\mathbf{B}^0, \mathbf{B}^1, \mathbf{B}^2, \mathbf{B}^3,$ and \mathbf{B}^4 are defined in Table 4.1. The basis matrices are generated using Equation 4.2 and 4.3. The SRVSS scheme makes use of these matrices to generate shares for this example. For this example follow the block pattern 1 as shown in Figure 3.4(a). This chapter makes use of same block pattern used by RVSS scheme in Chapter 3. Let us assume that, the secret image contains a white pixel then select basis matrix \mathbf{B}^0 . Now make random selection of row from \mathbf{B}^0 (say row 1). Assign the first column pixel 0 to share1, and so on to other shares. Now if the secret pixel is black and belongs to block A (first block from pattern 1), then choose the basis matrix \mathbf{B}^1 . Similarly, select random row for remaining block patterns and assign it to shares based on the pixel is black or white. Repeat the algorithm for each secret pixel to generate

Algorithm 4.1: Generation of shares using BPVSS scheme

Input: 1. The halftone image $\mathbf{SI}_{halftone}$ having size $W \times H$.
 2. Number of participants n
 3. The $n + 1$ basis matrices such that B^0, B^1, \dots, B^n

Output: The n shares : $\mathbf{SI}_i, i = 1, 2, \dots, n$ having size $W \times H$

```

1 for row ← 1 to W do
2   for column ← 1 to H do
3     Choose randomly number 1 or 2 and assign it to  $r$ 
4     for  $i \leftarrow 1$  to  $n$  do
5       Let  $Location(row, column) \in Block_m$  where Block follows one of
         the patterns as shown in Fig. 3.4
6         1: if  $\mathbf{SI}_{halftone}(row, column)$  is WHITE then
7           2:  $SI_i(row, column) \leftarrow B^0(r, i)$ 
8           3: else
9             4:  $SI_i(row, column) \leftarrow B^m(r, i)$ 
10          5: end if
        end
      end for
    end
  end for
end
    
```

four shares. The output of the BPVSS is four shares having same size as that of secret image **SI**. Figure 4.3 shows the four shares generated for the secret image **SI**.

4.1.2 Embedding secret image information into shares

Second phase of the SRVSS system is to embed the additional information about the secret image into shares. This chapter proposed to embed low resolution pixels into shares. Unlike RVSS (Mhala et al. 2018) scheme, this chapter embedded meaningful information instead of random pixel values. This chapter modified the RVSS scheme proposed in Chapter 3 to work with super-resolution to improve contrast of the recovered image. As scheme is embedding very few pixel value, it is hard to perceive the low resolution image directly from the shares. The RVSS scheme embedded the pixel data into the shares using DCT based reversible data hiding technique. To hide data into the shares, first transform shares into frequency domain using DCT. The frequency domain has the property that, changes made in middle frequency are less perceivable by human visual system. It means Human Visual System is less sensitive to the middle frequency change. Gujjunoori and Amberker (2013a,b) proposed the reversible data hiding technique for videos. Further, in RVSS scheme have used DCT based data hiding technique with modification for hiding pixel data. This chapter adapted data hiding technique used by RVSS scheme to embed pixel data into shares. Algorithm 4.2 shows the procedure used to embed data into shares. To embed the data, consider shares $(\mathbf{SI}_1, \dots, \mathbf{SI}_n)$ generated in above phase. The data hiding algorithm takes shares as input along with low resolution image. The low resolution image \mathbf{I}_{low} can be generated by down-sampling the secret image **I**. There exist many interpolation techniques to down-sample images like bi linear Smith (1981), bi-cubic Fadnavis (2014), etc. The SRVSS scheme used bi-linear interpolation to down-sample the secret image **SI**. This low resolution image will act as a cue for generating the super resolved image from shares. In order to embed the pixel data into shares, partition the shares $(\mathbf{SI}_1, \dots, \mathbf{SI}_n)$ into non-overlapping blocks $(\mathbf{C}_1^i, \mathbf{C}_2^i, \dots, \mathbf{C}_l^i)$ of size 8×8 . Here \mathbf{C}_l^i represents the l^{th} block of the i^{th} share. Where $i = 1, 2, \dots, n$ is the number of shares and $l = 1, 2, \dots, (w \times h)/64$ is the number of blocks for a share having size $w \times h$. These blocks \mathbf{C}_l^i are then transformed into frequency domain using Discrete Cosine Transform (DCT) as given in Equation 4.4.

4. Contrast enhancement of Random Visual Secret Sharing scheme

$$F_{u,v} = \frac{C(u) \times C(v)}{4} \sum_{s=0}^7 \sum_{t=0}^7 B_l^i(s, t) \times \bar{f}(s, t, u, v) \quad (4.4)$$

where $0 \leq u, v \leq 7$ and

$$\bar{f}(s, t, u, v) = \cos \frac{(2s+1)u\pi}{16} \cos \frac{(2t+1)v\pi}{16},$$

$$C(e) = \begin{cases} \frac{1}{\sqrt{2}} & e = 0 \\ 1 & e > 0 \end{cases}.$$

Algorithm 4.2: Embedding of data into shares

Input: All n shares as $\mathbf{SI}_1, \mathbf{SI}_2, \dots, \mathbf{SI}_n$
and low-resolution image

Output: Generates n shares of same size ($W \times H$) with embedded data.

- 1 Partition all shares into block of size 8×8 as $\mathbf{SI}_i = C_1^i, C_2^i, \dots, C_l^i$ where $1 \leq i \leq n$
- 2 **for** Each $C_j^i \in \mathbf{SI}_i$ where $1 \leq j \leq l$ **do**
- 3 Calculate the DCT of each C_j^i and then Quantize the DCT coefficients.
- 4 Let C_k ($1 \leq k \leq 9$) be the set of quantized coefficients of 8×8 each.
- 5 Let CJ_k be the number of continuous zeros from high frequency to low frequency in set D_k
- 6 **if** ($CJ_k \geq ((K(k)/2) - 1)$) **then**
- 7 Select the low-resolution pixel value that needs to be embedded for sets defined in Figure 3.5. Find the middle element position for set D^k as defined in Figure 3.5
- 8 $x = D^k(k, \lceil \frac{K(k)}{2} \rceil)$
- 9 // x contains the pixel value at the given location of set D^k
- 10 Resolve the Ambiguous condition using
- 11 $A \leftarrow \text{Amb}(x)$
- 12 Embed the value at location $D^k(k, \lceil \frac{K(k)}{2} \rceil)$ using
- 13 $E \leftarrow \text{Embed}(A, (\text{LRpixelvalues}))$
- 14 **end if**
- 15 **end**
- 16 **end for**
- 17 **end**

The DCT transforms spatial pixels of the image block into the frequency domain. To achieve better data embedding capacity, quantize the frequency coefficients using quantization table. Table 3.2 shows the standard quantization table used in this thesis for images. Please note that the quantization table is same that is used in Chapter 3 (Table 3.2). Algorithm 4.2 makes use of a Human Visual System (HVS) behavior to



Figure 4.4: (a) The embedded secret image information into the shares (b) The restored image by applying XOR operation on shares (\mathbf{SI}_{xor})

hide data into shares. The HVS system has the property that, it is less sensitive to the changes made in the middle frequency domain. Algorithm 4.2 uses middle frequency sets to efficiently embed data. The sets defined by the algorithm is same as used in Chapter 3 (Figure 3.5). Here there are total nine sets D^1, D^2, \dots, D^9 . These are the desired locations for hiding data into the block.

4.1.2.1 Pixel embedding procedure

Now consider set locations as shown in Figure 3.5 from Chapter 3 to embed data. Compute the number of ceaseless zero (CJ) present in each sets for high to low frequency coefficient. If $CJ_k \geq K(k)/2 - 1$ then fetch DCT coefficient value at middle location of sets $x = D^i(i, K(k)/2)$. The size of ceaseless zero $K(k)$ for each set is defined in Table 3.3. The sample ‘‘Lenna’’ image embedded into shares is shown is Figure 4.5(a).

Now before embedding value at desired location ambiguous conditions need to be resolved i.e. while extracting the pixel value one may encounter with the condition in which it is not clear whether the data is embedded or not. To resolve the ambiguous condition use function Amb given in Equation 4.5. The function $Embed$ is used to embed the actual pixel s into shares. The $Embed$ function takes output of function Amb along with pixel that needs to be embedded. In this chapter, the pixel value s is selected from the lexicographically ordered low resolution image vector. In case of RVSS



Figure 4.5: (a) The embedded secret image information into the shares (b) The restored image by applying XOR operation on shares (SI_{xor})

scheme selection of pixels were random pixel values within range of maximum and minimum pixel value for a given set. The SRVSS scheme has selected the meaningful pixels instead of random pixels which is further, used to improve the contrast of recovered image. The function Amb and $Embed$ used by algorithm is given by Equation 4.5 and 4.6

$$A = Amb(x) = \begin{cases} 0 & \text{if } x = 0 \\ x + 256 & \text{if } x \geq 1 \\ x - 256 & \text{Otherwise,} \end{cases} \quad (4.5)$$

$$E = Embed(A, s) = \begin{cases} s & \text{if } A = 0 \\ A & \text{Otherwise,} \end{cases} \quad (4.6)$$

4.1.3 Extraction of embedded data and low resolution image formation

This subsection focus on extraction algorithm used to extract hidden pixel data from shares and low resolution image formation to further enhance the quality of recovered image.

4.1.3.1 Extraction of embedded data from shares

Extraction of hidden pixel from shares is an inverse technique of embedding algorithm. Algorithm 4.3 describes the data extraction procedure used in this scheme. This chapter uses extraction algorithm used in the Chapter 3. Algorithm 4.3 takes n shares S_1, S_2, \dots, S_n as input and produces binary shares along with extracted pixel as output.

Algorithm 4.3: Extraction of data from shares and restoration of shares	
Input:	All n shares as S_1, S_2, \dots, S_n having size $W \times H$.
Output:	The n shares S_i with restored values and n marices containing Extracted Data E_i , where $i = 1, 2, \dots, n$
1	Partition all shares into block of size 8×8 as $S_i = C_1^i, C_2^i, \dots, C_l^i$ where $1 \leq i \leq n$;
2	for Each $C_j^i \in S_i$ where $1 \leq j \leq l$ do
3	Let $B_k (1 \leq k \leq 9)$ be the set of quantized coefficients of 8×8 each.
4	Let CJ_k be the number of continuous zeros from high frequency to low frequency in set B_k
5	if $(CJ_k \geq ((K(k)/2) - 1))$ then
6	Find the middle element position for set defined in Figure 3.5
7	$x = D^k(k, \lceil \frac{K(k)}{2} \rceil)$
8	Extract the information about embedded data using Equation 4.7
9	$E_i^j \leftarrow ExtractData(x)$
10	Restore the initial value at middle location using Equation 4.8.
11	$C_j^i \leftarrow Restore(x)$
12	end if
13	end
14	end for
15	end
16	Combine all the C_j^i such that $S_i = \{C_1^i, C_2^i, \dots, C_l^i\}$;
17	Combine all the E_j^i such that $E_i = \{E_1^i, E_2^i, \dots, E_l^i\}$;

Now, extract the data by partitioning the shares (S_1, \dots, S_n) into non-overlapping block ($C_1^i, C_2^i, \dots, C_l^i$) of size 8×8 . Now compute the ceaseless zero (CJ) for each set defined by embedding algorithm as shown in Figure 3.5. If total number of ceaseless zero for a set is less than or equal to defined number given in Table 3.3, then perform the extraction procedure on that set. Now select the middle element of a set using $x = D^i(i, K(k)/2)$. Once the value at middle location is fetched make use of function *Extract* to extract the hidden value. The *ExtractData* procedure is given in



Figure 4.6: (a) Recovered secret image information having size of 128×128 (b) The image used as initial guess to solve SR problem (c) The final restored image having size 512×512 in the gray-scale format

Equation 4.7. Once the pixel is extracted, restore the original values in order to compute inverse DCT. To restore the values make use of function *Restore* to restore the coefficient values as given in Equation 4.8. After the extraction of hidden pixels and restoration of original coefficient perform the inverse DCT on the shares to get back the original shares. Figure 4.6 (a) shows the recovered hidden image from the shares.

$$E = ExtractData(x) = \begin{cases} x & \text{if } 0 \leq x \leq 255 \\ 0 & \text{Otherwise,} \end{cases} \quad (4.7)$$

$$S = Restore(x) = \begin{cases} 0 & \text{if } 0 \leq x \leq 255, \\ x - 256 & \text{if } x \geq 256, \\ x + 256 & \text{Otherwise,} \end{cases} \quad (4.8)$$

4.1.3.2 The low resolution image formation

Once shares were restored using inverse DCT, apply XOR operation on restored shares **S1, S2, S3, S4** to recover the secret image SI_{xor} . The sample of secret image recovered after applying XOR operation on shares is shown in Figure 4.5 (b). The contrast of the secret image SI_{xor} is improved using MISR technique. In order to model the MISR problem, multiple low-resolution observations of the secret image are needed. The

L1, L2, and L3 low-resolution observations are used to super resolve the secret image SI_{xor} . The overview of the low resolution image formation is shown in Figure 4.7. The low-resolution image formation is discussed as follows:

1) **L1**: Figure 4.7(e) shows the first low-resolution image used with SRVSS scheme. Recalling from previous subsection 4.1.3, L1 is the extracted hidden image from the shares. L1 acts as cue to super resolve the secret image. L1 contains original pixels about the secret image. The dimension of L1 is 128×128 for the secret image “Lenna”.

2) **L2** :- Use reconstructed secret image SI_{xor} to form second low resolution observation (L2). Figure 4.7(f) shows the reconstructed secret image using XOR operations on shares $S1, S2, S3$, and $S4$. Now down-sample the secret image SI_{xor} by the factor of four to get low resolution image L2. The secret image SI_{xor} retains the high frequency information about the scene, like it holds the edge information of the secret image. While super resolving the secret image, low-resolution image L2 will act as cue to sharpen the edges of the final image.

3) **L3** :- It can be observed from the secret image SI_{xor} that it contains salt and pepper noise which arises while reconstructing the secret image. To reduce this noise (noise present in the image), apply the Gaussian blur on the secret image SI_{xor} . Now down-sample the blurred observation image by the factor of four. The image L3 is used to learn about the smooth region present in the original image.

Once multiple observations (three) about the secret image are formed, make use of popular super-resolution technique which reconstructs scene from blurred and down-sampled observations.

4.1.4 Contrast enhancement of recovered image using Super-resolution

The initial step in image restoration is to analyze and model the SR problem. In super-resolution, image restoration is achieved from various available low resolution observations. In general, restoration of image is considered as ill-posed problem, because of an insufficient number of low resolution images having ill-posed blur matrices. Typically, the formation of LR observations involves wrapping followed by blurring and down-sampling of the original HR image.

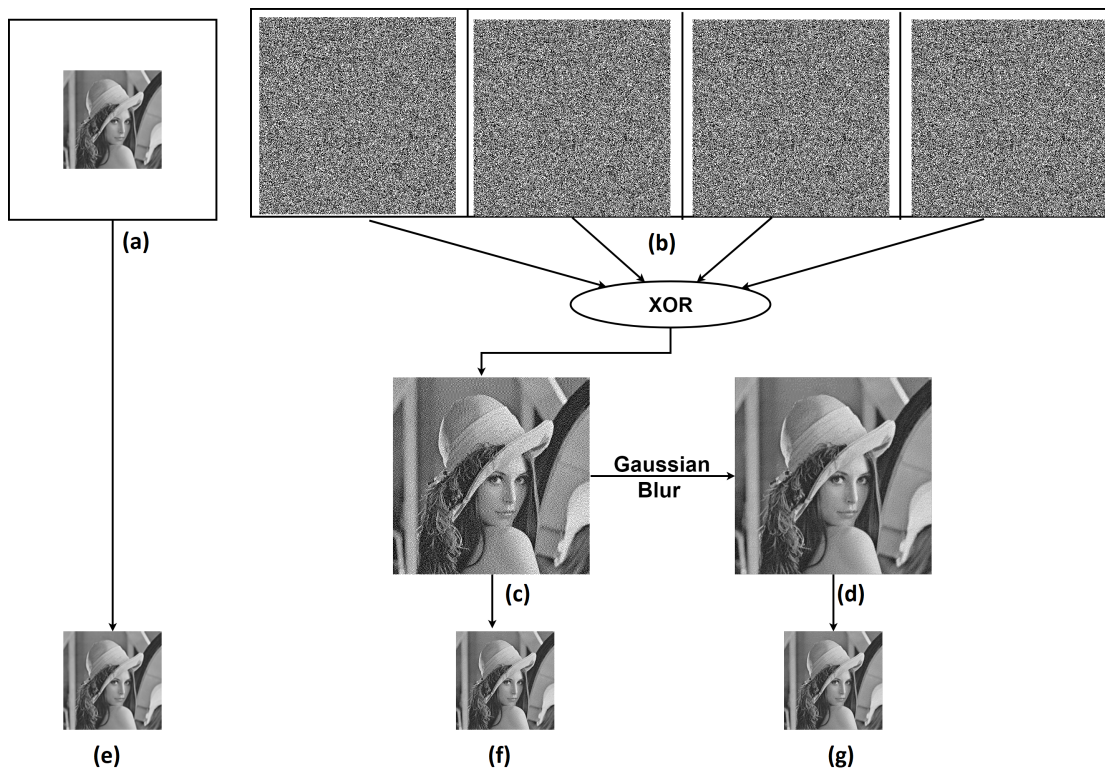


Figure 4.7: Overview of the low resolution image formation: (a) The extracted hidden image from shares (128×128) (b) The restored shares for four participants ($\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3, \mathbf{S}_4$) (512×512) (c) The recovered secret image (\mathbf{SI}_{xor}) by stacking shares $\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3, \mathbf{S}_4$ using XOR operation (512×512) (d) The image obtained after applying Gaussian blur on the \mathbf{SI}_{xor} image (512×512) (e) The first low resolution observation ($\mathbf{L1}$) (128×128) (f) The second extracted low resolution observation ($\mathbf{L2}$) (128×128) (g) The third low resolution image ($\mathbf{L3}$) (128×128).

The super-resolution restoration from linear blur, geometric wraps and additive noise has numerous applications in various fields. The proposed technique, takes advantage of super-resolution techniques, which have capability to restore scene from various low resolution observations. The proposed scheme adapted the popular super-resolution technique proposed by [Elad and Feuer \(1997\)](#). They proposed the image restoration technique which uses multiple low resolution observations to super resolve the scene. Let us, consider the basic super-resolution model as shown in Equation [4.9](#).

$$\underline{Y}_k = D_k C_k F_k \underline{X} + \underline{E}_k \quad \text{for } 1 \leq k \leq N \quad (4.9)$$

Where F_k represents the geometric wrap, C_k represents the blur matrix for k^{th} low resolution image, D_k is the decimation matrix and E_k is zero mean Gaussian additive noise for the k^{th} low resolution image. The Y_k is K^{th} the low resolution image. This technique, makes use of three low resolution images L1, L2, and L3 formed in previous section. The low resolution images ($L1, L2,$ and $L3$) formed are blurred, decimated and geometrically wrapped versions of HR image. Further, notation model can be grouped and simplified as follows.

$$\begin{bmatrix} \underline{Y}_1 \\ \vdots \\ \underline{Y}_N \end{bmatrix} = \begin{bmatrix} D_1 C_1 F_1 \\ \vdots \\ D_N C_N F_N \end{bmatrix} \underline{X} + \begin{bmatrix} \underline{E}_1 \\ \vdots \\ \underline{E}_N \end{bmatrix} = \begin{bmatrix} \underline{H}_1 \\ \vdots \\ \underline{H}_N \end{bmatrix} \underline{X} + \underline{E}$$

$$\underline{Y} = \underline{H}\underline{X} + \underline{E} \quad (4.10)$$

Equation [4.10](#) is the classic restoration problem model ([Gonzalez and Wintz 1977](#); [Jain 1989](#)). Now apply the Maximum a posteriori probability (MAP) estimator to restore the image \mathbf{X} . The MAP estimator is used to restore the high resolution image for given low resolution observations. The unknown SR image \mathbf{X} is restored by maximizing the conditional probability density function of ideal image with given observations $P\{\mathbf{X}|Y_1, Y_2, \dots, Y_k\}$. i.e.

$$\mathbf{X}_{MAP} = \arg \max_{\underline{X}} P(\underline{X}|Y_1, Y_2, \dots, Y_k) \quad (4.11)$$

From Bayes rule, it can be rewritten as given in Equation [4.11](#),

$$\mathbf{X}_{MAP} = \arg \max_{\underline{X}} \frac{P(Y_1, Y_2, \dots, Y_k|\underline{X}) P(\underline{X})}{P(Y_1, Y_2, \dots, Y_k)} \quad (4.12)$$

Since the denominator is not a function of \underline{X} , rewrite Equation [4.12](#) by deleting the

denominator and applying logarithm.

$$\mathbf{X}_{MAP} = \left(\sum_{k=1}^K \log P(Y_k|\mathbf{X}) + \log P(\mathbf{X}) \right) \quad (4.13)$$

$$P(Y_k|\mathbf{X}) = \frac{1}{C1} \exp \left(\frac{- \| D_k H_k F_k \mathbf{X} - Y_k \|^2}{2\sigma_k^2} \right) \quad (4.14)$$

Where $P(Y_k|\mathbf{X})$ is defined for the given model in Equation 4.14. Here C1 is constant and the σ is defined as error variance. Now modeling the prior image information in Gibbs form (Nasrollahi and Moeslund 2014; Rajan and Chaudhuri 2001) it will give Equation 4.15.

$$P(\mathbf{X}) = \frac{1}{C2} \exp(-\Gamma(\mathbf{X})) \quad (4.15)$$

Here C2 is a constant and $\Gamma(\mathbf{X})$ is the prior energy function. Now substituting Equation 4.14 and Equation 4.15 in Equation 4.13 to get MAP solution for SR problem as shown in Equation 4.16.

$$X = \arg \min_x (\| D_k H_k F_k X - Y_k \|^2 + \lambda \Gamma(\mathbf{X})) \quad (4.16)$$

Where first term $\| D_k H_k F_k X - Y_k \|^2$ is known as fidelity term, which measures the closeness of predicted HR image by solving problem with the captured LR images. The term $\Gamma(X)$ is the regularization term, which is used to achieve stable solution to problem. The regularization term is commonly used to compensate the missing measurement information with some general prior information about the desired HR solution. The scalar λ is used to balance the weight between fidelity term and regularization term known as regularization parameter. Now to define the prior image density $\Gamma(X)$. The widely used regularization functions for SR problems are Tikhonov-type regularizer (He and Kondi 2006; Lee and Kang 2003; Park et al. 2007; Patanavijit and Jitapunkul 2006, 2007) and Total Variance (TV)-type regularizer (Farsiu et al. 2004; Ng et al. 2007; Rudin et al. 1992). The SRVSS model uses Bilateral Total Variance (BTV) function as priors to improve estimation. The BTV regularization function for

the SR model is shown in Equation 4.17.

$$\Gamma(\mathbf{X}) = \sum_{l=-P}^P \sum_{m=0}^P \alpha^{|m|+|l|} \|X - S_x^l S_y^m X\| \quad (4.17)$$

Where S_x^l and S_y^m are the matrices (operators) obtained by shifting X by l and m pixels in horizontal and vertical direction respectively. The scalar weight α ($0 < \alpha < 1$), is imposed to provide spatially decaying effect to the summation of regularization terms.

$$\mathbf{X} = \arg \min_x \left[\sum_{k=1}^N \| D_k H_k F_k \mathbf{X} - Y_k \| + \lambda \sum_{l=-P}^P \sum_{m=0}^P \alpha^{|m|+|l|} \|X - S_x^l S_y^m\| \right] \quad (4.18)$$

The objective function used is shown in Equation 4.18. The cost function used is basically a minimization of data fidelity term for model given in Equation 4.9 and regularization term is minimization of BTV prior. There exist many algorithms to solve regularized SR problem such as Steepest Descent (SD), Gradient Decent (GD), Simulated Annealing (SA), etc. This chapter, used Conjugate Gradient (CG) optimization algorithm which usually converges much faster than SD (Bertsekas 1999; Nocedal and Wright 2006). The low resolution image recovered in previous step is considered as initial guess to provide better results. The initial guess image is constructed by up-sampling the hidden image using bilinear interpolation technique. The use of hidden image along with the available low resolution images provides the close estimation of final image. With the help of hidden data and SR technique with BTV prior, proposed scheme was able to improve the contrast and quality of the final image. The additional improvement in contrast is because, proposed scheme is hiding meaningful pixels information (low resolution image) instead of random pixel values (i.e. existing RVSS embeds random pixel values).

4.2 EXPERIMENTAL RESULTS

This section, compared the performance of the proposed VSS scheme with existing VSS schemes. Experiments were performed using Matlab 2015a running on Intel i7-4790 processor with 16GB RAM and Windows 10 operating system. The dataset (Hou 2012; of Southern California 1977) used to perform experimental results contain total

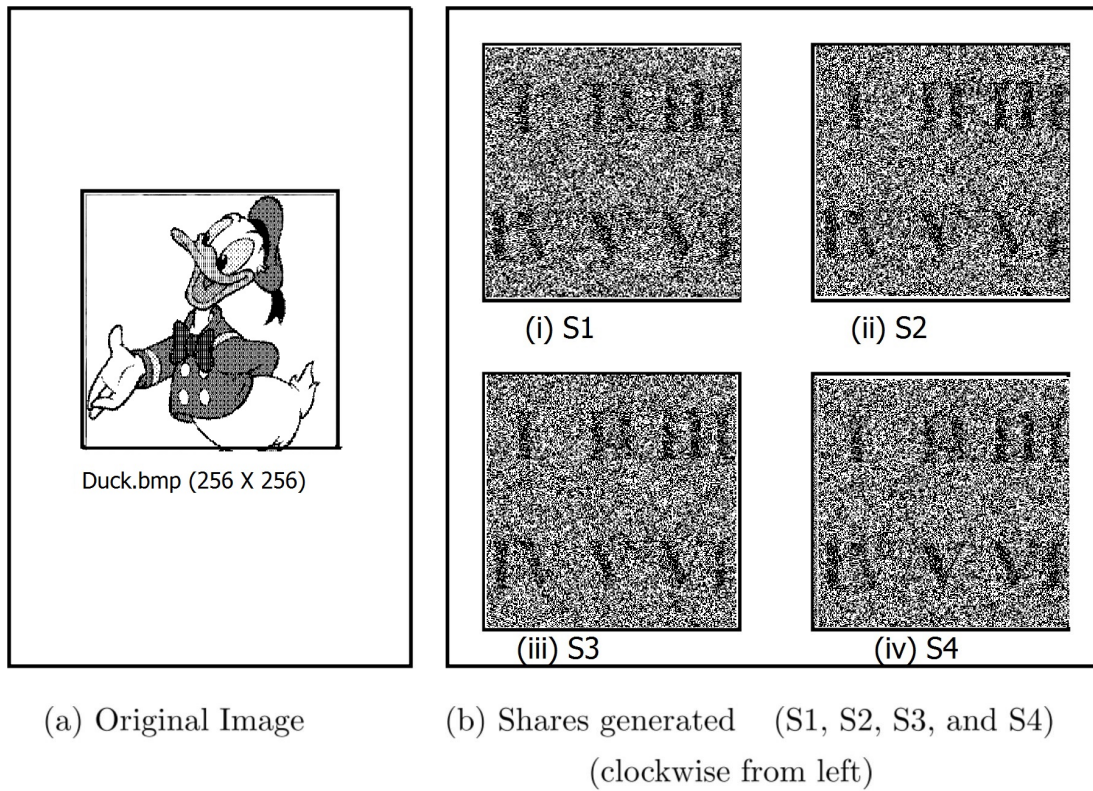


Figure 4.8: The sample shares generated for secret image: (a) The secret Image (b) The four meaningful shares generated for respective participants

of 42 images, 28 gray-scale and 16 color images. The sizes of the images are 256×256 (12 images), 512×512 (26 images) and 1024×1024 (4 images) respectively.

The presented system used two types of shares namely, (i) noise-like shares, and (ii) meaningful shares. The noise-like shares are the shares with random salt and pepper noise (Mhala et al. 2018), whereas meaningful share contains some visually meaningful cover image imposed on each share. Figure 4.3 and Figure 4.8 shows the types of shares used in this chapter. Figure 4.3 shows the four noise-like shares and Figure 4.8 shows the meaningful shares generated for the secret image.

The similarity between the secret image and recovered image is evaluated using popular metrics like Peak-Signal to Noise Ratio (PSNR), Normalized Cross-Correlation (NCC), Mean Square Error (MSE) and Normalized Absolute Error (NAE). The performance of the proposed system is compared with BPVSS and RVSS schemes. The test images used are shown in Figure 4.9 and Figure 4.10. Figure 4.9 shows four sample

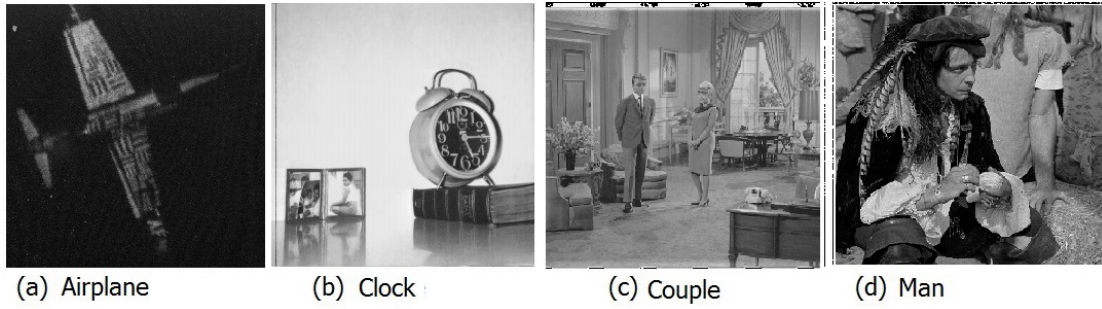


Figure 4.9: The sample test (gray-scale) images used by proposed system (a) Airplane, (b) Clock, (c) Couple, (d) Man

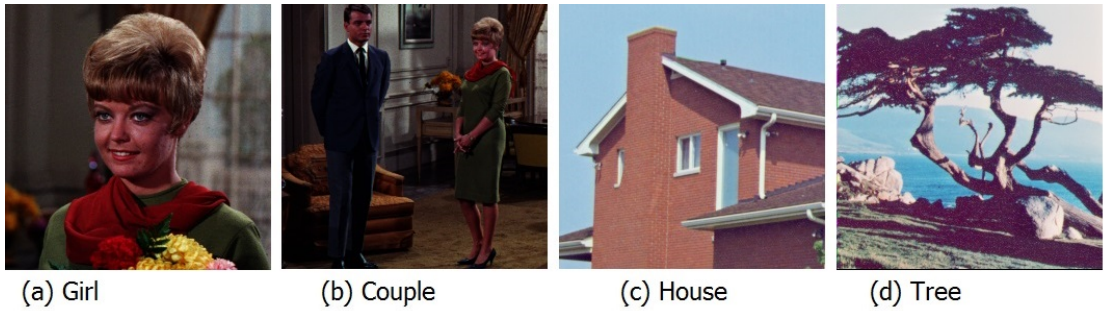


Figure 4.10: The sample test (Color) images used by proposed system (a) Girl, (b) Couple, (c) House, and (d) Tree

images (gray-scale) as (a) Airplane, (b) Clock, (c) Couple, and (d) Man. Similarly, Figure 4.10 shows the sample color images used in this chapter i.e., (a) Girl, (b) Couple, (c) House, and (d) Tree respectively.

Figure 4.7 shows the recovered LR images from shares. The initial guess is formed by up-sampling the hidden LR image. The initial guess used appears to be blurred, hence it suffers from problem of loss of sharp edges. As in SR technique we are adding the prior term as a cue to super-resolve secret image which sharpens the edges present in the secret images. Hence providing better contrast along with perceivable reconstruction of image by HVS.

4.2.1 Mean square error (MSE^{HVS})

Mean square error computes the cumulative squared error between the secret image and output image. The lower MSE values represent the better quality of the output image. MSE of the image takes values from 0 to 1. The MSE^{HVS} of the image is computed using Equation 4.19. From Table 4.2, it is observed that, the proposed scheme provides

Table 4.2: Mean square error-HVS value for various test images

Test Images	Size of Image	Type	RVSS (Mhala et al. 2018)		BPVSS (Hou et al. 2013a)		SRVSS (Mhala and Pais 2019a)	
			Noise-like	Meaningful	Noise-like	Meaningful	Noise-like	Meaningful
Girl	256	color	0.031	0.032	0.3945	0.4706	0.0018	0.014
Couple	256	color	0.018	0.016	0.4511	0.5328	0.0020	0.007
House	256	color	0.054	0.093	0.4987	0.5642	0.0017	0.049
Tree	256	color	0.05	0.107	0.1556	0.2456	0.0031	0.060
Airplane	256	gray-scale	0.048	0.071	0.4217	0.6107	0.0050	0.061
Clock	256	gray-scale	0.051	0.026	0.2451	0.5645	0.0050	0.024
Couple	512	gray-scale	0.023	0.11	0.4634	0.6577	0.0030	0.12
Man	1024	gray-scale	0.017	0.035	0.3201	0.6512	0.0030	0.034

values near to zero for recovered secret image. The secret image "Girl" from Table 4.2 is having the maximum value of 0.4706 for meaningful shares whereas proposed scheme provides the smaller error value of 0.0018 for meaningful color image.

$$MSE^{HVS} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [\mathbf{I}(i, j) - \mathbf{R}(i, j)]^2 \quad (4.19)$$

4.2.2 Peak-signal to noise ratio (PSNR)

PSNR of the recovered image is computed using Equation 4.20. It is computed as the ratio between maximum possible pixel value to the corrupting noise added in the original image. PSNR ratio is often used as the quality parameter between two images. Higher value of PSNR represent the better quality of recovered image in terms of HVS. PSNR is usually represented using logarithmic decibel scale. It can be observed from Table 4.3 that, for secret color image "Girl" having size 256×256 , BPVSS provides 54.9823 (dB) PSNR whereas RVSS provides better PSNR of 63.1850 (dB). Also it can be observe that, for same secret image using SR to recover secret images provides PSNR of 75.4609 (dB). Clearly, proposed scheme outperforms the existing VSS schemes in terms of PSNR values for both noise-like and meaningful shares.

$$PSNR = 10 \cdot \log_{10} \frac{255^2}{MSE^{HVS}}, (dB) \quad (4.20)$$

4.2.3 Normalized Cross-correlation (NCC)

NCC computes the similarity between two images. The higher value of NCC indicates the higher similarity between two images. The NCC can take values in the range of 0 and 1. For the secret image I and the recovered image R NCC is computed using Equation 4.21. It can be observe from Table 4.4 that existing RVSS scheme provides NCC values in the range of 0.640 to 0.906 for noise-like shares. Whereas, for meaningful shares RVSS scheme maintains the NCC values in the range of 0.526 to 0.807. The SRVSS scheme provides NCC values in the range of 0.9785 to 0.9990 for noise-like shares. The SRVSS scheme maintains NCC values in the range of 0.5899 to 0.773

Table 4.3: Peak signal-to-noise ratio (PSNR) value for various test images (in dB)

Test Images	Size of Image	Type	RVSS (Mhala et al. 2018)		BPVSS (Hou et al. 2013a)		SRVSS (Mhala and Pais 2019a)	
			Noise-like	Meaningful	Noise-like	Meaningful	Noise-like	Meaningful
Girl	256	color	63.185	63.02	54.9823	48.3780	75.4609	66.731
Couple	256	color	65.692	65.958	54.3289	47.8261	73.7315	69.627
House	256	color	60.786	58.45	55.3641	47.1272	74.9455	61.213
Tree	256	color	61.15	57.828	56.2114	49.6327	72.8695	60.366
Airplane	256	gray-scale	61.339	59.623	54.0019	46.8364	70.9150	58.623
Clock	256	gray-scale	61.088	64.062	54.2374	50.6142	70.8170	65.072
Couple	512	gray-scale	64.44	57.717	55.3217	51.7624	72.8010	58.89
Man	1024	gray-scale	65.755	92.694	55.3654	49.4328	73.0330	64.82

Table 4.4: Normalized Cross Correlation (NCC) value for various test images

Test Images	Size of Image	Type	RVSS (Mhala et al. 2018)		BPVSS (Hou et al. 2013a)		SRVSS (Mhala and Pais 2019a)	
			Noise-like	Meaningful	Noise-like	Meaningful	Noise-like	Meaningful
Girl	256	color	0.777	0.718	0.4998	0.2489	0.9785	0.754
Couple	256	color	0.703	0.701	0.4879	0.2484	0.9498	0.773
House	256	color	0.798	0.641	0.5010	0.2479	0.9959	0.582
Tree	256	color	0.853	0.671	0.4435	0.2364	0.9932	0.682
Airplane	256	gray-scale	0.640	0.526	0.5002	0.2498	0.9930	0.5899
Clock	256	gray-scale	0.815	0.574	0.5001	0.2483	0.9990	0.5878
Couple	512	gray-scale	0.792	0.730	0.4987	0.2503	0.9950	0.6952
Man	1024	gray-scale	0.906	0.807	0.5003	0.2481	0.9970	0.5986

for meaningful shares. Also it can be observed from Table 4.4 that, presented scheme provides almost 99% of contrast for the noise-like shares and almost same contrast as RVSS for meaningful shares. The presented scheme outperforms the existing RVSS scheme providing maximum possible contrast up to 99% for noise-like shares, while retaining meaningful shares contrast.

$$NCC = \sum_{i=1}^X \sum_{j=1}^Y \frac{\mathbf{I}_{i,j} \cdot \mathbf{R}_{i,j}}{\mathbf{I}_{i,j}^2} \quad (4.21)$$

4.2.4 Normalized absolute error (NAE)

NAE indicates the error between a secret image I and a recovered image R . The lower NAE implies the better quality of recovered image. The NAE is computed using Equation 4.22. Table 4.5 shows the NAE values for recovered images using BPVSS scheme, RVSS scheme and proposed scheme. It can be observed from Table 4.5 that the values are near to zero for the proposed system as compared to the existing RVSS and BPVSS scheme. Also, for meaningful images the NAE values are better than BPVSS and nearly similar for RVSS scheme.

$$NAE = \sum_{i=1}^X \sum_{j=1}^Y \frac{\mathbf{I}_{i,j} - \mathbf{R}_{i,j}}{\mathbf{I}_{i,j}} \quad (4.22)$$

4.2.5 Structural Similarity Index (SSIM)

Structural Similarity Index (SSIM) (Wang et al. 2004) is the image quality metric, which computes the similarity between two images. The SSIM mainly computes three terms such as contrast, luminance and structural terms. For two similar images SSIM will be near to one and similarly, for dissimilar images it is near to zero. For secret image I and recovered image R , SSIM is given by Equation 4.23.

$$SSIM(x, y) = [l(x, y)]^\alpha \cdot [c(x, y)]^\beta \cdot [s(x, y)]^\gamma \quad (4.23)$$

Where,

$$\begin{aligned} l(x, y) &= \frac{2\mu_x\mu_y + C1}{\mu_x^2 + \mu_y^2 + C2} \\ c(x, y) &= \frac{2\sigma_x\sigma_y + C2}{\sigma_x^2 + \sigma_y^2 + C2} \\ s(x, y) &= \frac{\sigma_{xy} + C3}{\sigma_x\sigma_y + C3} \end{aligned}$$

where $\sigma_x, \sigma_y, \mu_x, \mu_y$, and σ_{xy} are the local standard deviations, means, and cross-covariance for images x, y . For $\alpha = \beta = \gamma = 1$ and $C3 = C2/2$, SSIM can be simplified as fol-

Table 4.5: Normalized Absolute Error (NAE) value for various test images

Test Images	Size of Image	Type	RVSS (Mhala et al. 2018)		BPVSS (Hou et al. 2013a)		SRVSS (Mhala and Pais 2019a)	
			Noise-like	Meaningful	Noise-like	Meaningful	Noise-like	Meaningful
Girl	256	color	0.65	0.616	0.5010	0.7502	0.1285	0.263
Couple	256	color	0.245	0.263	0.4989	0.7492	0.2344	0.341
House	256	color	0.372	0.431	0.5001	0.7498	0.0519	0.224
Tree	256	color	0.364	0.494	0.5002	0.7153	0.0780	0.286
Airplane	256	gray-scale	0.252	0.399	0.5002	0.7510	0.3960	0.258
Clock	256	gray-scale	0.259	0.155	0.5001	0.7487	0.0680	0.359
Couple	512	gray-scale	0.255	0.124	0.4967	0.7485	0.0820	0.289
Man	1024	gray-scale	0.262	0.38	0.4998	0.7498	0.1120	0.392

4. Contrast enhancement of Random Visual Secret Sharing scheme

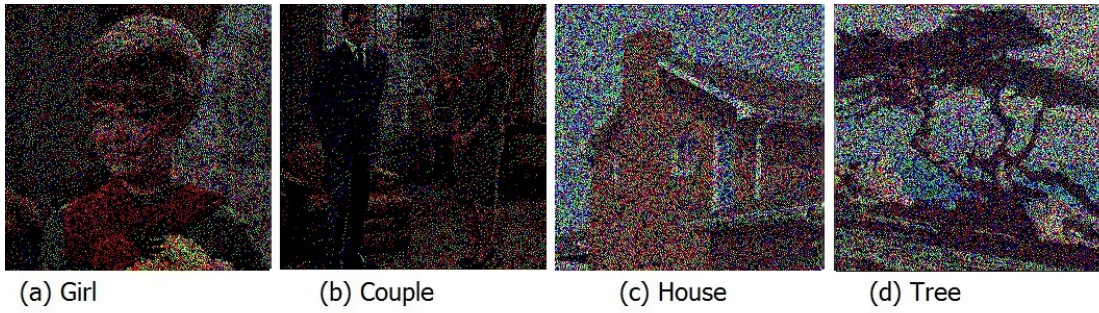


Figure 4.11: The sample outputs of BPVSS scheme (Color images) (a) Girl (b) Couple, (c) House, and (d) Tree

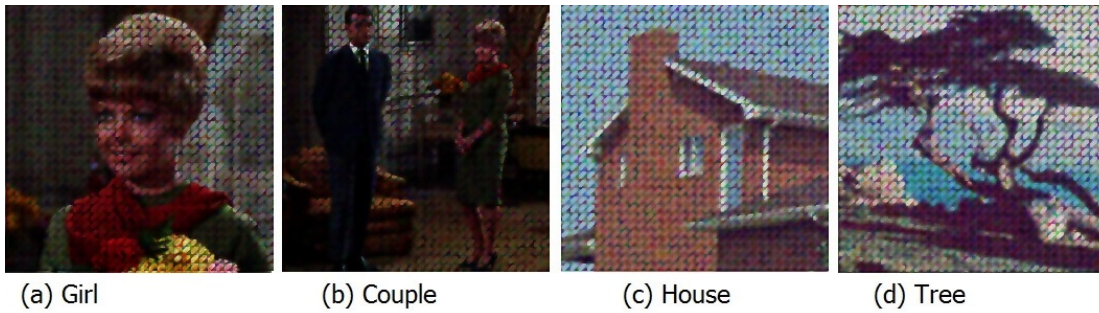


Figure 4.12: The sample outputs of RVSS scheme (color images) (a) Girl (b) Couple, (c) House, and (d) Tree

lows.

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C1)(2\sigma_{xy} + C2)}{(\mu_x^2 + \mu_y^2 + C1)(\sigma_x^2 + \sigma_y^2 + C2)} \quad (4.24)$$

It is evident from the Table 4.6 that the SRVSS scheme outperforms other schemes for noise-like shares and provides almost similar result for the meaningful shares. For the noise-like image "Girl" the RVSS and BPVSS provides 0.6850 and 0.6256 SSIM respectively. Whereas, the SRVSS scheme provides 0.8005 SSIM.

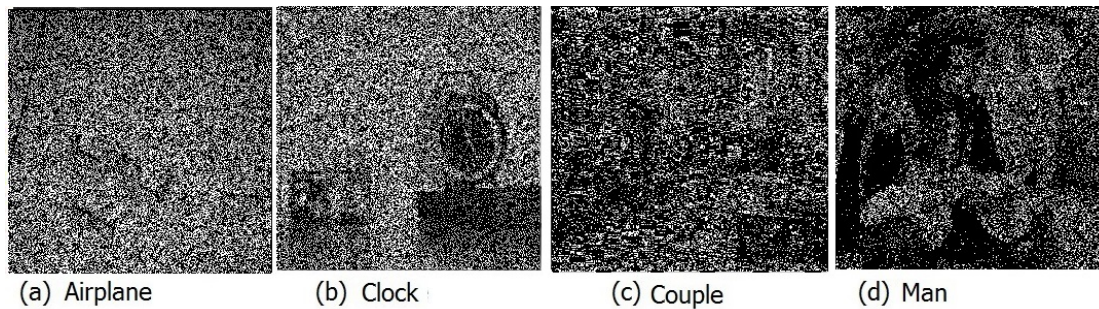


Figure 4.13: The sample outputs of BPVSS scheme for gray-scale images (a) Airplane, (b) Clock, (c) Couple, and (d) Man

Table 4.6: Structural Similarity Index (SSIM) value for various test images

Test Images	Size of Image	Type	RVSS (Mhala et al. 2018)		BPVSS (Hou et al. 2013a)		SRVSS (Mhala and Pais 2019a)	
			Noise-like	Meaningful	Noise-like	Meaningful	Noise-like	Meaningful
Girl	256	color	0.6256	0.2218	0.685	0.0080	0.8005	0.3094
Couple	256	color	0.7104	0.4104	0.1534	0.0785	0.7135	0.4964
House	256	color	0.3375	0.0524	0.0432	0.0017	0.6688	0.0874
Tree	256	color	0.4041	0.0882	0.1016	0.0015	0.7778	0.1468
Airplane	256	gray-scale	0.8262	0.6547	0.5437	0.0108	0.8264	0.6624
Clock	256	gray-scale	0.2458	0.0945	0.0643	0.0015	0.4645	0.0932
Couple	512	gray-scale	0.4485	0.1661	0.3834	0.0010	0.7632	0.1617
Man	1024	gray-scale	0.7222	0.5284	0.7940	0.0198	0.9465	0.5363

4. Contrast enhancement of Random Visual Secret Sharing scheme

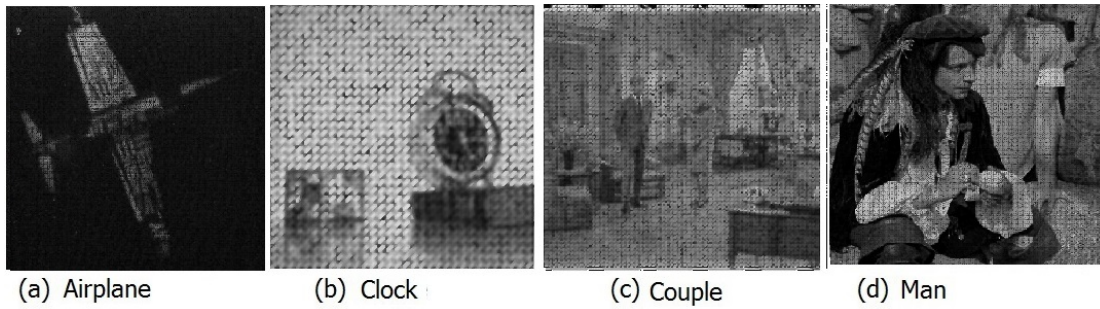


Figure 4.14: The sample outputs of RVSS scheme for gray-scale images (a) Airplane, (b) Clock, (c) Couple, and (d) Man

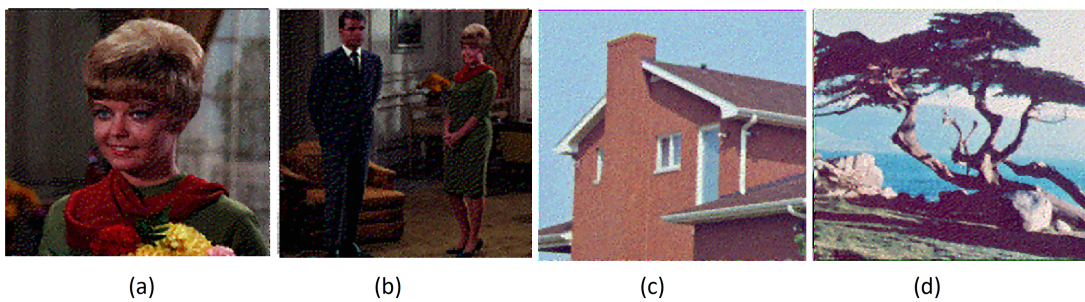


Figure 4.15: The sample output of the SRVSS scheme for color images (a) Girl, (b) couple, (c) House, and (d) tree

The sample of the reconstructed secret image using BPVSS scheme for color and gray-scale images is shown in Figure 4.11 and Figure 4.13. It is evident from Figure 4.11 and Figure 4.13 that BPVSS generates noisy output images as compared to the RVSS scheme. The secret image constructed using the RVSS scheme for gray-scale and color images are shown in Figure 4.14 and Figure 4.12 respectively. Although RVSS reconstructs secret image with improved contrast as compared to BPVSS, it still contains blocking artifacts in the final output images (Figure 4.14 and Figure 4.12). Whereas, the SRVSS scheme reconstructs secret image with a better contrast and also removes blocking artifacts too. The sample output images reconstructed using the SRVSS scheme are shown in Figure 4.16 and Figure 4.15 respectively.

The BPVSS scheme provides the contrast of 50% for noise-like gray-scale images whereas, RVSS scheme provides the recovery of a secret image with better contrast of upto 70-90%. But it is evident from the experimental results, that proposed scheme outperforms over other available schemes. The SRVSS scheme achieves 99% of contrast for recovered images. Also the RVSS scheme generates blocking artifacts while recov-

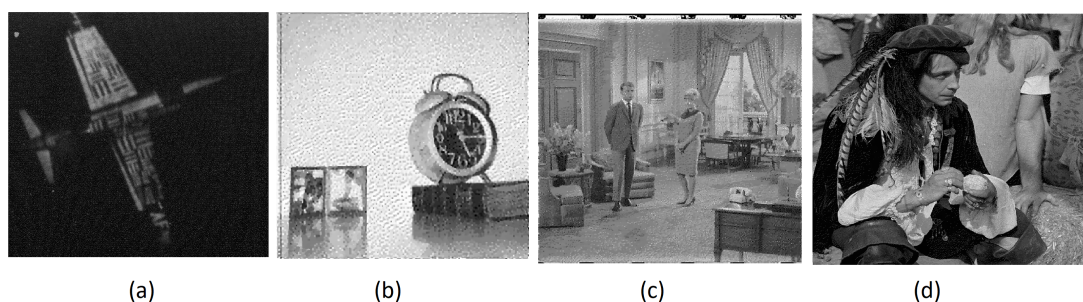


Figure 4.16: The sample output of the SRVSS scheme for gray-scale images (a) airplane, (b) clock, (c) couple, and (d) man

ering the image. The blocking artifact are the result of random pixel values embedded into shares resulting in sudden change at the middle location. The SRVSS scheme used the meaningful pixels instead of random pixels to improve the quality of image. As scheme is embedding very few pixel values into shares proposed scheme is secure. One can not get entire information about secret image with available embedded data. The SRVSS scheme recovers the secret image with almost 99% contrast. Also SRVSS scheme does not posses any blocking artifact in the recovered images (Figure 4.16 and Figure 4.15).

4.3 SUMMARY

This Chapter presented a novel super-resolution based VSS scheme for gray-scale and color images. The SRVSS scheme improves the visual quality and contrast of the RVSS scheme presented in Chapter 3. The SRVSS scheme embeds the low-resolution information about the secret image into shares. The super-resolution is a popularly used area in the field of image processing. The super-resolution technique extracts features from multiple low-resolution images to form a single high dimensional image. This chapter, has adapted the concept of Super-resolution to improve visual quality of the VSS scheme. The use of low-resolution information instead of randomized pixel values adds the more visual information into the reconstructed image, which further improves the contrast and visual information quality of the secret image at the receiver end. The experimental results shows that, the SRVSS scheme is able to reconstruct secret image with a better contrast of 70-90% for noise-like shares and almost 99% for meaningful shares respectively.

CHAPTER 5

APPLICATIONS OF THE VISUAL CRYPTOGRAPHY

Nowadays medical information is being shared over the communication networks due to ease of technology. The patient's medical information has to be securely communicated over the network for Computer Aided Diagnosis (CAD). Most of the communication networks are prone to attacks from an intruder thus compromising the security of patients data. Therefore, there is a need to transmit medical images securely over the network. Visual secret sharing scheme can be used to transmit the medical images over the network securely. Visual Secret Sharing (VSS) scheme generates multiple shares to share secret information among n participants. To recover the secret information, all shares should be stacked together. Chapter 3, presented a VSS based technique to recover secret images with the contrast of 70-80% known as Randomized Visual Secret Sharing (RVSS) scheme. However, RVSS scheme suffers from problems like 1) Generation of blocking artifacts in the recovered images. 2) The RVSS scheme recovers medical images with a maximum contrast of 30-40%, hence it is not suitable for medical images.

This chapter makes use of modified RVSS scheme to recover the medical images with improved contrast. The presented scheme applies the idea of using super-resolution concept to improve the contrast of reconstructed medical images. The reconstruction quality of the medical images is evaluated using Human Visual System (HVS) based parameters. Additionally, the performance of the presented system is evaluated using the existing Computer Aided Diagnosis (CAD) systems. The experimental results showed

that the presented system is able to reconstruct the secret image with the contrast of almost 85-90% and similarity of almost 77%. Also, the reconstructed images using the presented system achieves the similar classification accuracy as that of existing CAD systems.

5.1 THE SECURE VISUAL SECRET SHARING (VSS) SCHEME FOR MEDICAL IMAGES

The Internet becomes the necessary tool in daily life to transfer digital information. As the Internet is publicly available, it is vulnerable to attacks from an intruder. Recently, many organizations or businesses have gradually paid attention to the issue of information security due to continuous occurrences of an intrusion event. Hence, how to protect the security of digital information has become a major challenge.

Nowadays processing and handling of medical data by computers over the network have become common practice by hospitals. Hence, there is a need to transmit medical data securely over the network to facilitate diagnosis of patients disease. However, unauthorized people can easily intrude the medical information system and steal important information. Hence there is a need to transmit medical information securely.

Recently, [Mhala et al. \(2018\)](#) proposed a VSS scheme which addresses the problems of BPVSS scheme. The scheme is also referred as Randomized Visual Secret Sharing (RVSS) scheme (Chapter [3](#)). This scheme proposed the contrast improvement in the recovered image using the data hiding technique. The RVSS scheme hides the pixel information about the secret image into the shares. Also, RVSS scheme recovers the secret image in the multitone format. Although the RVSS scheme recovers the image with better contrast, it suffers from a problem of a blocking artifact generation. The generation of blocking artifact in the reconstructed images, makes the RVSS scheme inefficient for Computer Aided Diagnosis (CAD) systems. Hence, there is a need to improve the contrast of the recovered image and make it suitable for a CAD system. Chapter [4](#) proposed an super-resolution based VSS scheme, that have improved the contrast of the secret image and also removed the blocking artifacts from the secret image.

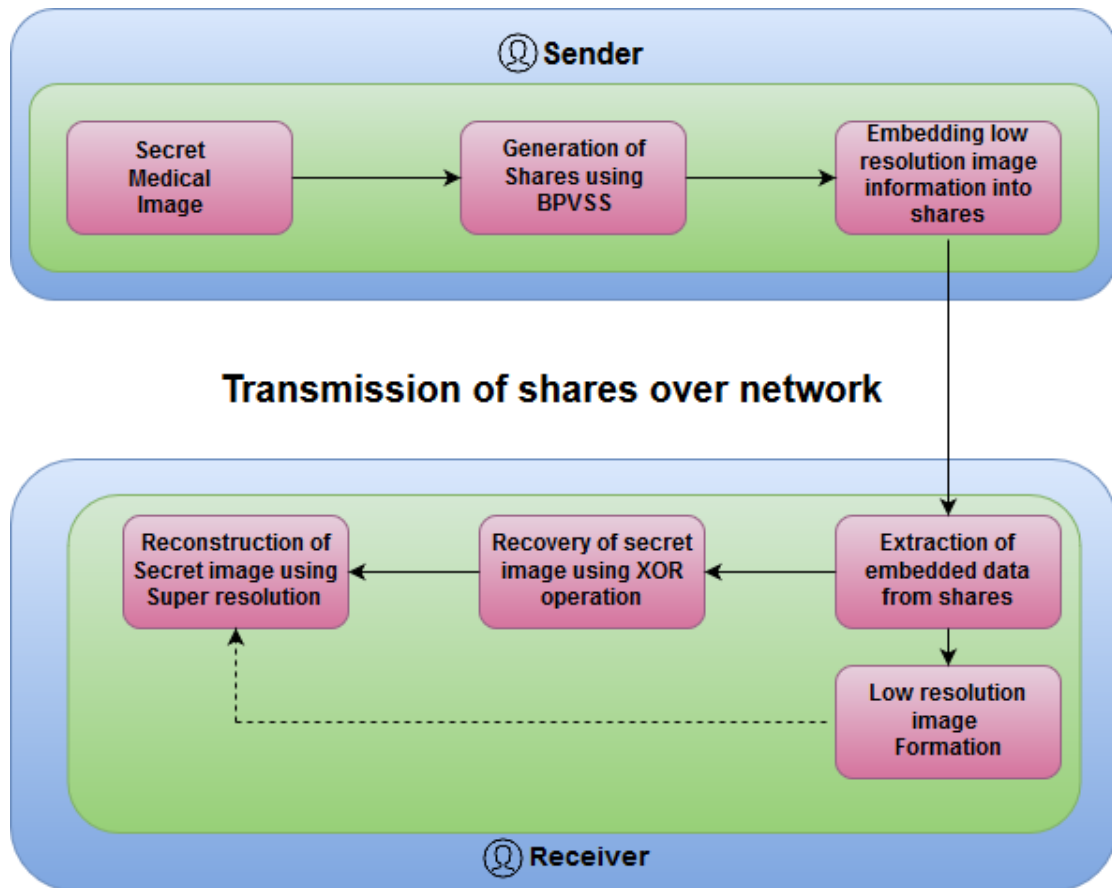


Figure 5.1: The overview of the proposed system

5.2 VSS SCHEME FOR MEDICAL IMAGES

This chapter, makes use of an improved and secure VSS scheme for medical images presented in Chapter 4. The overview of the proposed system is shown in Figure 5.1. The proposed system mainly consists of two modules namely the sender module and the receiver module. The sender module contains the following steps 1) Generation of shares using BPVSS. 2) Embedding low-resolution image information into shares. Whereas, the receiver module contains the following steps 3) Extraction of embedded data from shares. 4) Recovery of the secret image using XOR operation. 5) Low resolution image formation and finally 6) Contrast enhancement of the recovered image using Super resolution technique. These steps used in medical images are explained below.

5.2.1 Generation of shares using BPVSS

The first stage in the proposed system is to generate n shares for the secret medical image. Generation of shares is achieved with the help of BPVSS scheme. The BPVSS scheme has a property that, it can progressively recover the secret image with a maximum contrast of 50%. The algorithm used for the generation of shares is given in Algorithm 4.1. It takes a halftone ($SI_{halftone}$) image as input to generate n shares. The halftone technology transforms the multitone image into the binary image while preserving the visual property of the image. This chapter used same Floyd-Steinberg Error Diffusion (Floyd 1976) method to generate a halftone image as used in Chapter 4. The algorithm also takes basis matrices as input along with halftone image $SI_{halftone}$. The basis matrices are the collection of zeros and ones which are used to mask secret image pixels. For the n participants, total $n + 1$ matrices of size $2 \times n$ were generated. Please note that, the basis matrices used in this chapter are same as that used in Chapter 4. The basis matrices are shown in Table 4.1. The first row in the basis matrix B^0 is filled with all zeros and second row of the matrix is all ones. The matrix B^0 is used to mask the white pixel of the $SI_{halftone}$ image. For masking the black pixel, remaining n matrices were generated in this chapter. The first row of the matrix is initialized to zeros, and the second row is initialized to one, except bit values at n^{th} location has been toggled for all n matrices (i.e., for B^1 first column is toggled, for B^2 second column is toggled, and for B^n n^{th} column is toggled).

To generate shares, logically partition the secret medical image ($SI_{halftone}$) into m blocks. Here m is equal to the number of blocks defined by users. The proposed work used two block patterns as shown in Figure 3.4 (i.e., for Figure 3.4 (a) $m = 4$ and for Figure 3.4 (b) $m = 4$). Now if the black pixel of the secret image belongs to m^{th} block then, select the respective basis matrix (i.e., B^m) to generate shares. Similarly, for a white pixel, replace shares pixel using basis matrix B^0 as given in Algorithm 4.1. It is observed from Algorithm that, selection of rows from basis matrices is random, which avoids the formation of duplicate shares. Hence makes the scheme more secure.

5.2.2 Embedding low-resolution image information into shares

The second stage in the sender module is to embed the low-resolution pixel information into shares. The idea is to use these hidden pixels to improve the contrast of the secret recovered image. Embedding of low-resolution information into shares is achieved using the Discrete Cosine Transform (DCT) based data hiding techniques (Gujjuroori and Amberker 2013a,b). The proposed approach adapted the data hiding technique used by RVSS and SRVSS scheme. The application discussed in this chapter embeds low-resolution medical image in to shares. The procedure for embedding the low-resolution information is given in Algorithm 4.2.

To embed the pixel data, divide shares into blocks of size 8×8 . To hide data into shares first, transform the shares into the frequency domain using DCT. The frequency domain has the property that, changes made in the middle frequency are less perceivable by Human Visual System (HVS). It means HVS is less sensitive to the middle frequency change. Now make use of HVS property to hide pixel data into the shares. The data hiding algorithm takes BPVSS shares as input along with the low-resolution medical image. The low-resolution medical image can be generated by down-sampling the secret medical image. The low-resolution image formation is discussed separately in the upcoming subsection 5.2.5. In order to embed the pixel values use the nine sets (D^1, D^2, \dots, D^9) as defined in Figure 3.5. To embed pixel data apply DCT on each block of shares which transform the spatial share into the frequency domain. Once shares are transformed into frequency domain, quantize each block with a standard quantization table. To embed the pixel values, first find out the trail of zeros in the middle frequency locations. The location that has a trail of zeros in the middle frequency of each block is used to hide low-resolution pixel data. Once the embedding is done, transmit these shares over the network to individual participants.

5.2.3 Extraction of embedded data from shares

The extraction mechanism is the inverse procedure of data embedding algorithm. The algorithm used for extraction of embedded data from shares is given in Algorithm 4.3. In order to extract the hidden data, first partition the shares into blocks of size $8 \times$

8. Now for each block B^i and set k ($1 \leq k \leq 9$), count the ceaseless zeros. If number of ceaseless zeros are greater or equal to $\frac{K(k)}{2} - 1$ (Table 3.3), then extract the hidden pixel information from the middle frequency of the desire set. To extract the pixel information, make use of procedure *ExtractData* given in Equation 5.1. Once the pixel values are extracted from each share, the hidden low-resolution image gets revealed. Now restore the original DCT coefficient values using the Equation 5.2. The function *Restore* restores back the initial coefficient values of shares. Now de-quantize the restored shares by multiplying it with the same quantization table and apply inverse DCT to get the original BPVSS shares.

$$E = ExtractData(x) = \begin{cases} x & \text{if } 0 \leq x \leq 255 \\ 0 & \text{Otherwise,} \end{cases} \quad (5.1)$$

$$D = Restore(x) = \begin{cases} 0 & \text{if } 0 \leq x \leq 255, \\ x - 256 & \text{if } x \geq 256, \\ x + 256 & \text{Otherwise,} \end{cases} \quad (5.2)$$

5.2.4 Recovery of the secret image using XOR operation

Once shares are restored and hidden pixel values are being extracted, now recover the secret image. The equation used for recovery of shares ($S_1, S_2 \dots S_n$) is given in Equation 5.3.

$$SI_{xor} = S_1 \oplus S_2 \dots \oplus S_n \quad (5.3)$$

To recover the secret medical image, stack shares using a simple *XOR* operation. The recovered image using *XOR* operation is a binary image and contains the random salt and pepper noise. Hence, there is a need to enhance the quality of the recovered image. In order to improve the quality of the recovered secret image, make use of a hidden low-resolution information. As per Chapter 4 to improve the quality of the secret medical image using SR, one need to form multiple low-resolution images. The multiple low-resolution image formation for medical image is discussed in the section 5.2.5 separately before using Multiple Image Super Resolution (MISR).

5.2.5 Low resolution image formation

This subsection, discusses the low-resolution image formation for medical image. First, form the secret low resolution image by down-sampling the secret medical image by the factor of four. This is the same down-sampled image that was embedded into shares as explained in subsection [5.2.2](#). Extract the embedded low-resolution from shares as explained in subsection [5.2.3](#). The extracted low-resolution medical image (LR1) acts as first low-resolution observation. Since proposed scheme used the reversible data hiding scheme, it recovers the same embedded image. Now more information about the secret medical image can be learned from the recovered image (i.e., using XOR). The recovered image is in the halftone format, but it preserves the high-frequency component, which mostly contains edge or shape information of nucleus of the medical image. In order to use this information, down-sample the recovered image by the factor of four, which will act as a second low-resolution image (LR2) observation. The recovered image using *XOR* mostly contains the salt and pepper noise. In order to minimize the salt and pepper noise, apply the Gaussian filter on the recovered secret medical image. Here 3×3 size Gaussian filter is used for all the medical images. The smoothed image after applying filter can be used to formulate third low-resolution image (LR3) observation. To model low-resolution image down-sample the smoothed image by the factor of four. Once three low-resolution images (LR1, LR2 and LR3) are formed, use it to enhance the recovered image. The contrast enhancement of the medical image using these three low-resolution observation is explained in sub subsection [5.2.6](#). The low-resolution images depict the visual information about the secret image which can be used as a cue to reconstruct the secret medical image.

5.2.6 Contrast enhancement of the recovered image using Super Resolution

The Chapter [3](#), presented contrast enhancement of the recovered image using the random hidden pixel values. This chapter used modified RVSS ([Mhala and Pais 2019a](#)) scheme to improve the quality and contrast of the secret medical image using super resolution. Super resolution is a technique mostly used to obtain one or more high-resolution images from one or more low-resolution image. This chapter used Multiple

Image Super Resolution (MISR) to improve the quality of the secret medical image. In the previous section, the low-resolution observations of the secret medical image (LR1, LR2 and LR3) were formed. Now make use of these low-resolution images to improve the quality and contrast of the recovered image. The initial step in solving the super resolution problem is to model the SR problem. This chapter consider the basic SR model as shown in Equation 5.4.

$$\underline{Y}_k = D_k C_k F_k \underline{X} + \underline{E}_k \quad \text{for } 1 \leq k \leq N \quad (5.4)$$

Here F_k denotes the geometric wrap, C_k denotes blur matrix for k^{th} low-resolution image, D_k is the decimation matrix and E_k is zero mean Gaussian additive noise. Here chapter used the three low-resolution images formed in the previous step to super resolve recovered image. SRVSS adapted the super resolution technique proposed in Elad and Feuer (1997) to restore the image from several blurred, noisy, and geometric wrapped images. Also this chapter used MAP-BTV based approach to solve the SR problem. The objective function used in this chapter is shown in Equation 5.5

$$X = \arg \min_x \left[\sum_{k=1}^N \left\| D_k H_k F_k X - Y \right\| + \lambda \sum_{l=-P}^P \sum_{m=0}^P \alpha^{|m|+|l|} \|X - S_x^l S_X\| \right] \quad (5.5)$$

The first term $\| D_k H_k F_k X - Y \|$ shown in Equation 5.5 measures the closeness of predicted HR images by solving problem iteratively. The second term $\alpha^{|m|+|l|} \|X - S_x^l S_X\|$ is regularization which provides the stable solution to the SR problem. Here S_x and S_X are the matrices obtained by shifting X by l and m pixel. α is the scalar which adds decaying effect to the cost function. This scheme used Scaled Conjugate Gradient (SCG) optimization algorithm to minimize objective function. The scheme considered $\lambda = 0.1$ for the experimentation. The use of low-resolution images formed in the previous step works as a cue to SR the recovered secret medical image. The existing RVSS scheme hides the random pixels into the shares, which results in addition of blocking artifact into recovered images. The use of low-resolution images ensures a

better estimation of the secret medical image using SR. The reconstructed secret medical image is similar to secret image, which can be use for the CAD system. Figure 5.2 shows the output image after applying super resolution on the recovered image.

5.3 EXPERIMENTATION RESULTS

The proposed system is evaluated for efficiency and reconstruction quality with existing VSS based scheme (Mhala et al. 2018). Section 5.3.1 shows the reconstruction quality of the medical image in terms of HVS based parameters. Section 5.3.2 shows that proposed system can be used for the CAD system.

5.3.1 The visual quality of the reconstructed image

In this section the quality of the reconstructed image has been evaluated with the help of HVS based parameters. The reconstructed image was compared with the existing RVSS technique. All experimentation were performed on the system having Intel i7 processor and 16Gb RAM. For the experimentation scheme used Matlab 2015a having computer-vision toolbox as development tool. The breast cancer dataset (dat 2015) was used for experimentation. The dataset contains a total 361 images. The dataset is categorized into three classes namely 1) Normal (119 samples) 2) Ductal carcinoma in situ (102 samples) and 3) Invasive carcinoma (140 samples). The proposed system was evaluated using Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Normalized Cross Correlation (NCC), Normalized Absolute Error (NAE), and Structural Similarity Index (SSIM). From the Table 5.1 it is evident that the proposed system outperforms the RVSS scheme. The proposed scheme achieves the contrast of 84% (average of all images), whereas RVSS is able to recover secret image with the contrast of 35%. Also, the proposed scheme recovers the secret medical image with similarity of up to 70% (average of all images) as compared with RVSS (similarity $\leq 10\%$).

Table 5.1: The average values of HVS parameters for all medical images

Method	MSE	PSNR	NCC	NAE	SSIM
RVSS	0.0551	60.7458	0.2024	0.3019	0.0601
Proposed System	0.0020	75.5495	0.8416	0.0510	0.6988

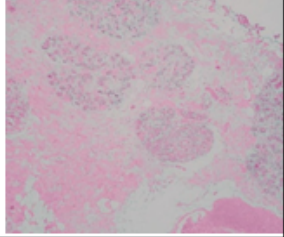
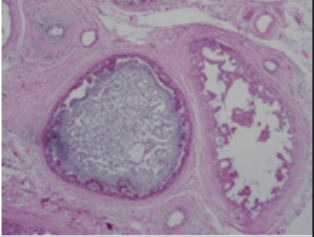
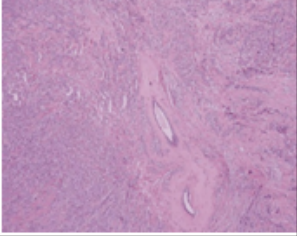

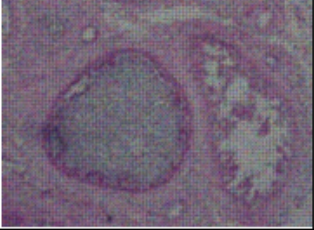

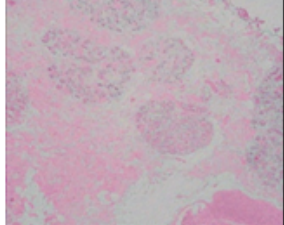
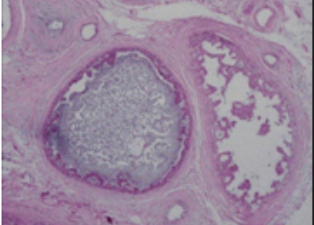
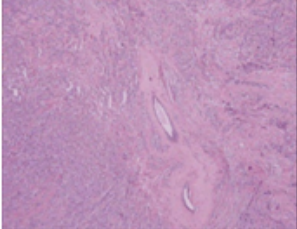
	Normal Sample	Carcinoma in Situ Sample	Invasive Carcinoma Sample
Test Images			
RVSS Scheme			
Proposed System			

Figure 5.2: Sample test images used for experimentation and the reconstructed images using RVSS (Mhala et al. 2018) and proposed scheme

5.3.2 The performance of the proposed system for Computer Aided Diagnosis (CAD)

The performance of the proposed system for CAD is evaluated using popular bag-of-feature (BOF) method (Bhandari 2015; Cruz-Roa et al. 2011; Mhala and Bhandari 2016). The classification of histopathology images using BOF is performed using following steps:-

1. **Feature extraction :-** Two types of feature extraction methods namely Scale Invariant Feature transformation (SIFT) (Lowe 2004) and Discrete Cosine transformation (DCT) are considered for the experimentation. The SIFT mainly contains following steps 1) Scale-space extrema detection from series of Difference-of-Gaussian (DOG) images obtained from the secret image. 2) Identification of strong interest point location among the potential key-points obtained in the previous step. 3) Assign the orientation to the key-points. 4) Compute the rotation

invariant descriptor using orientation. This application used the 128 dimension vector (8 orientation for 4×4 block) to represent SIFT feature points. DCT is computed on a block size of 8×8 . DCT computes the cosine coefficients for each block. The coefficients obtained by applying DCT represents the energy of the image. The DCT was applied on each R, G, and B plane separately, hence it formed the feature vector of 192 dimensions.

2. **Codebook construction :-** The codebook construction (Csurka et al. 2004) step is used to model the visual dictionary. To form the codebook use the k-means clustering algorithm. The k-means clustering is used to reduce the dimensionality of the extracted features. This scheme has clustered the extracted features into clusters of size 300, 500, and 1000.
3. **Bag-of-feature representation of image :-** Now represent the image using the histograms. The histogram for image contains bins equal to the number of clusters. The more clusters represent more unique histogram for an image. Hence increase in cluster improves the classification performance of the system.
4. **Classification of image :-** Finally, to predict the class of a test image this scheme has used multi-class Support Vector Machine (SVM) classifier. The breast cancer images are classified into three classes namely, 1) Normal samples 2) Ductal carcinoma in situ, and 3) Invasive carcinoma.

The presented system was evaluated for performance with existing CAD system using BOF approach for SIFT and DCT features. The proposed system was compared with 1) BOF approach on original images (BOFOI), and 2) recovered images using RVSS scheme (RVSSI). It can be observed from Table 5.2 and 5.3 that proposed scheme achieves the similar accuracy as that of BOFOI after cluster size of 500 and 1000 for SIFT features. Similarly, for cluster size of 300 with DCT based features the proposed scheme achieves the similar accuracy of BOFOI.

Additionally, the performance similarity of the proposed system using Sensitivity, Specificity, Precision, Recall and F-measure with BOFOI and RVSSI is shown in

Table 5.2: BOF approach with SIFT features (300 and 500 clusters)

	RVSSI	BOFOI	Proposed system	RVSSI	BOFOI	Proposed system
	300 clusters			500 clusters		
Accuracy	0.25352	0.91079	0.84037	0.24883	0.92019	0.88263
Sensitivity	1	0.84906	0.71698	1	0.81132	0.62264
Specificity	0.00325	0.93125	0.88125	0	0.95625	0.96875
Precision	0.25000	0.80357	0.66667	0.24883	0.86000	0.86842
Recall	1	0.84906	0.71698	1	0.81132	0.62264
F-Measure	0.4000	0.82569	0.69091	0.39849	0.83495	0.72527

Table 5.3: BOF approach with SIFT features (1000 clusters)

	RVSSI	BOFOI	Proposed system
Accuracy	0.42253	0.89671	0.89671
Sensitivity	0	0.79245	0.69811
Specificity	0.56250	0.93125	0.96250
Precision	0	0.79245	0.86046
Recall	0	0.79245	0.62264
F-Measure	0.38978	0.69811	0.72527

Table 5.4: BOF approach with DCT features (300 and 500 clusters)

	RVSSI	BOFOI	Proposed system	RVSSI	BOFOI	Proposed system
	300 clusters			500 clusters		
Accuracy	0.27230	0.99061	0.99530	0.28638	0.99530	0.99530
Sensitivity	1	0.98148	0.98148	1	1	1
Specificity	0.03125	1	0.99371	0.05000	0.99375	0.99375
Precision	0.25480	1	0.98148	0.25853	0.98148	0.98148
Recall	1	0.98148	0.98148	1	1	1
F-Measure	0.40613	0.99065	0.98148	0.41085	0.99065	0.99065

Table 5.2 and 5.3 for 300, 500, and 1000 clusters respectively for SIFT features. The results showed that BOFOI with SIFT feature achieves the accuracy of 92.09% for cluster size of 500. Whereas, the proposed system achieves the accuracy of 88.92%. Also BOF with SIFT for cluster size of 1000, the proposed scheme achieves the similar accuracy as that of BOF of 89.67%. It can also be observed that the proposed system with DCT feature achieves the classification accuracy of 99.53% for cluster size of 300, 500 and

Table 5.5: BOF approach with DCT features (1000 clusters)

	RVSSI	BOFOI approach	Proposed system
Accuracy	0.24882	0.99531	0.99531
Sensitivity	1	0.98148	0.98148
Specificity	0	1	1
Precision	0.24882	1	1
Recall	1	0.98148	0.98148
F-Measure	0.39849	0.99069	0.99069

1000 (Table 5.4 and Table 5.5). Also it is evident that BOF with DCT features are better than the SIFT for the proposed system and BOFOI. Hence the proposed VSS scheme for medical images can be used for secure transfer of medical images over the network and computer aided diagnosis.

5.4 THE SECURE VISUAL SECRET SHARING SCHEME FOR UNDERWATER IMAGES

An underwater image contains the different types of objects like minerals, metals, etc. (Glasby 2000; Halfar and Fujita 2007) which is often considered as an important resource/information. As these images contain valuable information, it needs to be transmitted securely over a network. Nowadays, researchers proposed various schemes to detect salient objects present in an image. Recently, Fu et al. (2019) proposed a generalized Convolution Neural Network (CNN) architecture namely “Deepside” to detect salient objects present in an image. They have fused the hierarchical CNN features using the segmentation based pooling. Most of the neural network based technique suffers from the problem of coarse object boundaries. To solve this problem Zhao et al. (2019) proposed an Edge Guidance Network (EGNet) technique. They have three main stages in EGNet as: 1) The first stage extracts the salient object features. 2) The second stage integrates the local and global edge information and 3) The third stage couples the same salient edge features with salient object features at various resolutions. A novel Joint Learning and Densely-cooperative Fusion (JL-DCF) architecture for RGB-D salient object detection are proposed in Fu et al. (2020). They have used RGB and depth channels jointly to learn about the salient objects using a Siamese network. Further, in Fan et al.

(2020) authors provided a new dataset and benchmarks to explore the salient object detection area.

The Visual Secret Sharing (VSS) scheme is a cryptography technique, which divides the secret image into multiple shares. These shares are then transmitted over a network to respective participants. To recover the Secret Image (SI), all participants must have to stack their shares together at the receiver end. The advantages of the VSS scheme over the traditional cryptography techniques are as follows:

- The VSS schemes do not require any knowledge of very complex algorithms to recover SI. It only needs to stack multiple shares together to recover the SI
- The SI is divided into multiple shares, which provides additional security by ensuring that, all participants must come together to recover the SI
- The adversary alone cannot recover the SI without acquiring all the shares
- The shares generated have a noise-like appearance, which alone cannot reveal any information about the SI

Naor and Shamir (1994a) proposed a VSS scheme for sharing binary images. They have masked binary pixels as a combination of a white and black pixel. To recover the secret binary image, they have used a simple + (OR) operation. Although the scheme proposed by Naor and Shamir (1994a) recovered SI, it was still restricted to binary images only and also suffers from the problem of pixel expansion. Pixel expansion in the VSS scheme increases the size of the recovered SI by expanding the original pixels. Hou et al. (2013a) proposed the Block-based Progressive Visual Secret Sharing (BPVSS) scheme to recover gray-scale and color images. The VSS scheme proposed by Hou et al. (2013a) recovered SI without any pixel expansion. They have also recovered SI block by block (i.e., progressively). Their work also proposes a technique, which recovers the SI like a jig-saw puzzle. They have recovered the SI in the halftone format instead of a multitone format. Still, it can recover SI with at-most 50% contrast.

Recently, proposed Randomized VSS (RVSS) (Mhala et al. 2018) scheme recovered the SI with a better contrast of 70-80%. It also recovered the SI in the multitone

format. Although RVSS recovered the SI with a contrast of 70-80%, it suffered from various problems like 1) Addition of blocking artifact, which was due to the use of hidden random pixel values to recover the SI. 2) It was not suitable for complex images like medical (Mhala and Pais 2019b) and underwater images. Hence to solve these problems Chapter 4, proposed to use a super-resolution (SR) technique to improve the reconstruction quality of the SI. This chapter have proposed a secure VSS scheme to transmit underwater images over a network. To the best of our knowledge, there is not much work done to transmit underwater images securely using VSS. The main contributions of the thesis to transmit underwater images over the network are:

- Presented a novel super-resolution based progressive VSS scheme to transmit underwater images securely over a network
- Presented a CNN-based architecture to reduce various artifacts present in the reconstructed image
- Presented CNN architecture, leveraged the CNN to extract the residual image from the SI to improve the visual quality of the image

5.5 THE SUPER-RESOLUTION BASED VISUAL SECRET SHARING (SRVSS) SCHEME

This subsection provide a brief description of the Super-resolution (SR) based VSS (SRVSS) scheme. VSS is a scheme that shares the secret visual information among n users. The overview of the SRVSS is depicted in Figure 5.3. The proposed system is divided into two modules: 1) Generation of shares by the sender and 2) Reconstruction of secret information at the receiver end. In the sender module, the sender first generates multiple shares using the BPVSS scheme (Hou et al. 2013a) as a pre-processing step. The multiple shares were generated for underwater images using BPVSS scheme. The algorithm used for generation of shares is same as that of medical image application. The BPVSS algorithm is shown in Algorithm ???. The BPVSS share generation algorithm is explained in subsection 5.2.1. Here this underwater image application uses same BPVSS algorithm to generate shares. Four shares generated for underwater image

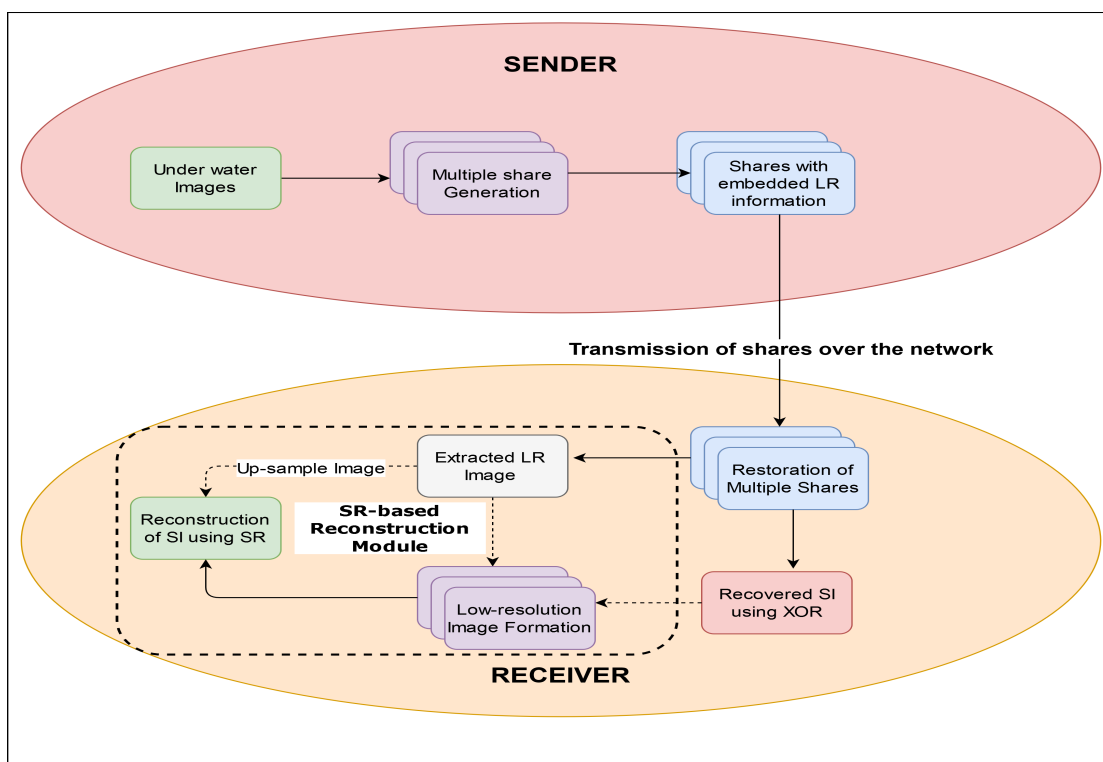


Figure 5.3: The Overview of the Super-resolution based VSS scheme for transmission of underwater images

5.5. The Super-resolution based Visual Secret Sharing (SRVSS) Scheme

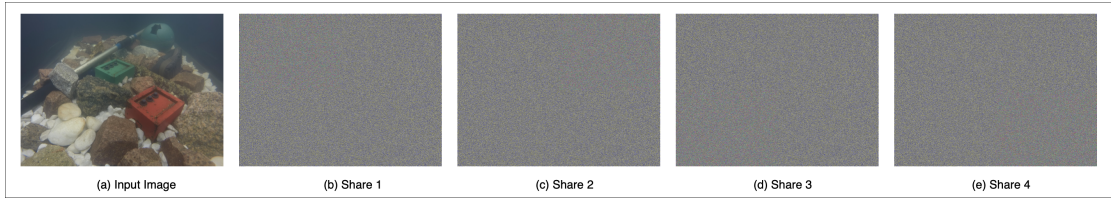


Figure 5.4: Four shares generated by the proposed technique for the input image (for $n = 4$ participants) (a) Original input image, (b-d) shares generated for 4 participants

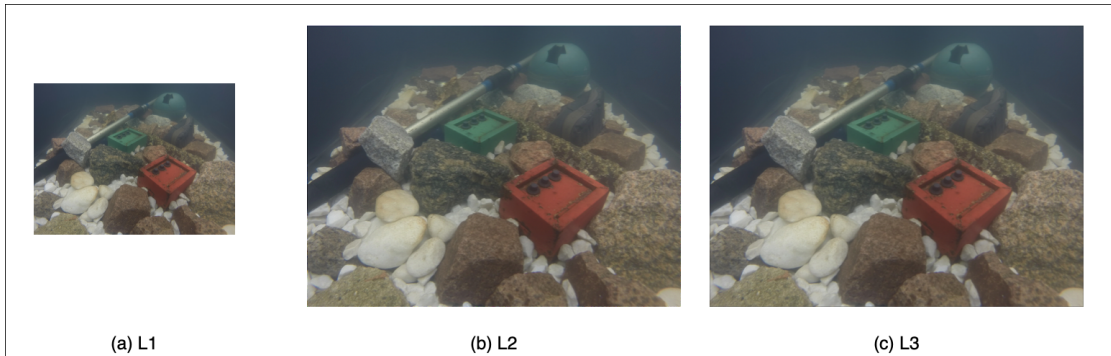


Figure 5.5: Low-resolution image formation (a) The L1 observation: extracted from the shares. (b) The L2 observation: formed by stacking the restored shares together, and (c) The L3 observation: obtained by applying Gaussian blur on L2

using BPVSS scheme is shown in Figure 5.4. Once multiple shares are generated, next step in SRVSS is to embed the Low-resolution (LR) information about the SI into the shares, and these shares are then transmitted to the participants over the network. The procedure used by underwater application to form LR images is same as explained in subsection 5.2.5. Figure 5.5 shows the low-resolution images formed for an underwater image. Whereas, at the receiver side, first extract the LR information and restore the multiple shares. Once shares are restored, SI is recovered using a simple XOR operation. Now generate the multiple LR images from the extracted LR image and the recovered image. Figure 5.5(a) shows the original LR image embedded into the shares, Figure 5.5(b) shows the L2 observation formed by stacking BPVSS shares together, and Figure 5.5(c) shows the L3 observation formed after applying Gaussian blur on the L2 observation. These LR image observations are further used to super resolve the recovered image to reconstruct the final SI. The reconstruction of the secret underwater image using SR from L1, L2, and L3 is explained in the following subsection.

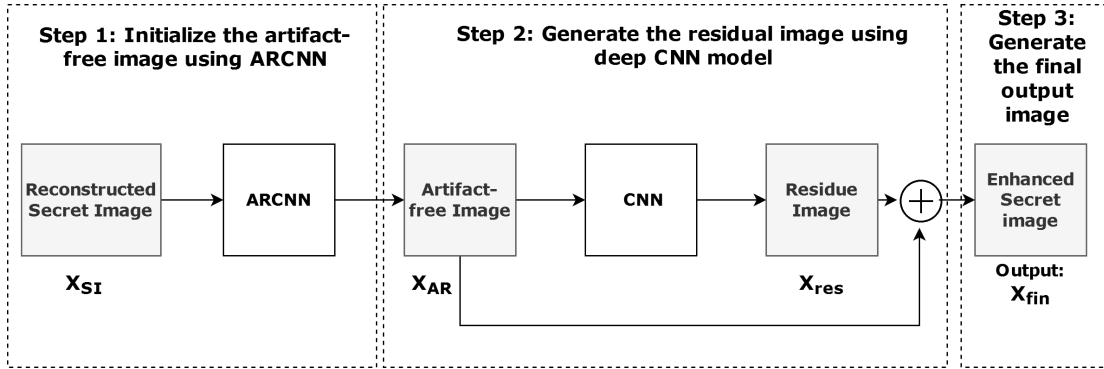


Figure 5.6: The proposed CNN-based image enhancement architecture for SRVSS

5.5.1 Reconstruction of the secret underwater image using SR

The underwater image application used same SRVSS technique discussed in subsection 5.2.6 to improve the quality and contrast of underwater images. SR is a technique that makes use of one or more LR images to construct a high-resolution (HR) image. There are two types of super-resolution techniques, namely (1) single image SR (SISR) and (2) multiple image SR (MISR). SISR uses only one LR image to reconstruct the HR image. Whereas MISR uses multiple LR images to reconstruct HR image. The SRVSS scheme uses MISR to reconstruct the HR image. The SRVSS scheme makes use of the above L1, L2, and L3 observation formed for underwater image as shown in Figure 5.5 to reconstruct the HR image with improved quality and without the blocking artifacts. The underwater application has considered the same basic SR model as given in Equation 5.5.

The first part in Equation 5.5 is the data fidelity term, and the second term represents the regularization term, which uses BTV prior to improve the reconstruction of the HR image. Here, S_x^l and S_m^y are the operators obtained by shifting X by l and m pixels in the horizontal and vertical directions, respectively. There exist many algorithms to solve minimization problems like gradient descent (GD), steepest gradient (SD), simulated annealing (SA), etc. the underwater image application has used the conjugate gradient (CG) optimizer, which converges faster than SD (Bertsekas 1999; Nocedal and Wright 2006). The extracted LR image (L1) from shares is considered as an initial guess, which is similar to the HR image in order to get a good HR image estimation. The HR

underwater image formed using LR images is free from blocking artifact.

5.6 IMAGE ENHANCEMENT USING CONVOLUTION NEURAL NETWORK

This section discusses a CNN-based architecture to enhance the visual quality of the reconstructed secret image. Although the proposed SRVSS reconstructed the secret image with better visual quality, it still suffers from various types of artifacts like ringing effect, blocking artifacts, and blurring effect along the edges. The underwater application proposed to reduce various artifacts present in the SRVSS scheme by adding a residue image into the noise-free image. The main steps of the architecture proposed for image enhancement using CNN are shown in Figure 5.6. The proposed architecture contains three steps such as 1) Initialize the artifact-free image using ARCNN (Dong et al. 2015), 2) Generate the residual image using a deep CNN model, and 3) Generate the final output image. Each step of the proposed system is discussed in detail as follows.

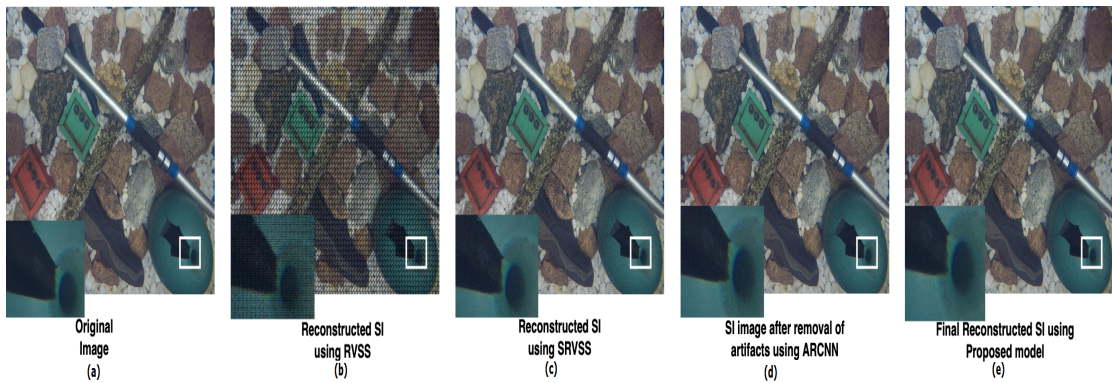


Figure 5.7: A sample output for reconstruction of secret Chlorophyll (Font view) underwater image. (a) The original underwater image, (b) Reconstructed underwater image using the RVSS scheme, (c) reconstructed underwater image using the SRVSS scheme, (d) the underwater image after removal of artifacts using ARCNN, and (e) final reconstructed underwater image using CNN-based VSS scheme. (The original image too large for display, hence only part of an image is shown for better visualization)

5.6.1 Initialize the artifact-free image using ARCNN

The use of SR to reconstruct the SI introduces additional artifacts into the final image. From Figure 5.7 (c), it is observed that the image contains the ringing effect along the

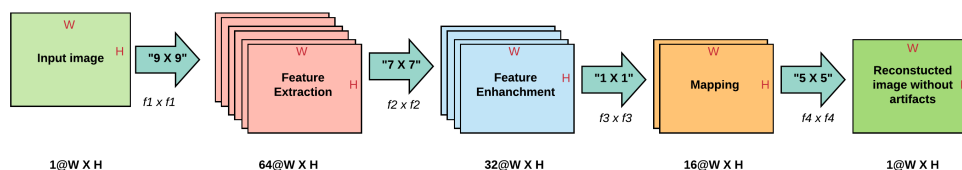


Figure 5.8: Overview of the ARCNN architecture for removal of artifacts

edges. Also, a reconstructed image contains blocking artifacts and blurring effects due to the loss of high-frequency components. Although different approaches are being proposed to reduce blocking artifacts, blurring effect, and ringing effect, they all work with a specific type of artifacts. Hence there is a need to propose a technique to remove all these artifacts.

Recently, proposed technique by [Dong et al. \(2015\)](#) namely, Artifacts Reduction Convolution Neural Networks (ARCNN), reconstructs the image free from the above artifacts. They have proposed a technique to reduce various artifacts, that arises in compressed JPEG images. It is observed that the reconstructed SI also contains similar types of artifacts. Hence the ARCNN technique has been used as an initialization step to generate a better quality image.

The ARCNN uses a simple four-layer architecture to remove artifacts from a given image. The architecture used by ARCNN technique is shown in [Figure 5.8](#). The ARCNN technique is based on the Super-Resolution Convolutional Neural Network (SRCNN) model of [Dong et al. \(2016\)](#), which uses simple convolution layers. The SRCNN model uses three convolution layers for the reconstruction of the LR image. The ARCNN adds the feature enhancement layer after feature extraction. As shown in [Figure 5.8](#), the first layer in the ARCNN is feature extraction layer. The first layer extracts the features from the input image by using filter of size 9 and outputs total 64 features for a input image. However, there are various artifacts coupled together with extracted features. Hence it contains the noisy observations; in order to reduce these noisy observations, the second layer defined as feature enhancement is introduced in the architecture. The second layer uses filter of size 7×7 to extract 32 feature enhanced images. After the second layer, the remaining layers are the same as that of SRCNN

(Dong et al. 2016). The third CNN layer does the mapping, and the final layer reconstructs the artifact-free observation of the input image. The layer three used filter size of 1×1 to map the features. Finally output is generated by applying filter size of 5×5 to get artifact free image as a pre-processed image. The underwater application system has used filters of size 9-7-1-5 (Dong et al. 2015) for the removal of artifacts from the secret underwater image. ARCNN is used as an initialization step to generate an artifact-free image. Generated output image helps the proposed model to learn and generate a better residual image for a given SI.

5.6.2 Generate the residual image using deep CNN model

Many researchers (Dian et al. 2018; Timofte et al. 2013, 2014; Zeyde et al. 2010) stated that the use of a residual image as a prior improves the reconstruction quality of the image. Residual learning greatly helps the CNN network in speeding up the training and also boosts up the learning performance of the system. The CNN techniques have achieved state-of-the-art performance in the area of image classification (He et al. 2016), and image denoising (Zhang et al. 2017). This proposed deep CNN network is motivated by the concept that the addition of a residual image to the low-resolution image works as a prior to improve the visual quality of the image. This scheme followed the generalized very deep CNN model having 16 blocks. The various blocks used in the deep CNN network are as follows:

1. *[Convolution + ReLU] (CR)*: The very first block of the network uses 64 filters of size 3×3 .
2. *[Convolution + Batch Normalization + ReLU] (CBR)*: The block number 2 to 15 also uses 64 filters with a kernel size of 3×3 . Additionally, the Batch normalization layer is added in these blocks to accelerate the training process.
3. *[Convolution] (C)*: The last block contains 64 filters of size 3×3 , which generates the final residue image for a given image.

5.6.3 Generate the final output image

The previous step generates a residual image (X_{res}) for a given image X_{AR} . Make use of the learned X_{res} image to generate the final output image. The final output is generated using Equation 5.6. The X_{res} learned by a proposed deep CNN, acts as a cue to improve the overall quality of the final image. The final output image generated by the proposed architecture retains the better high-intensity pixels along the edges while preserving the smoothness of the image.

$$X_{fin} = X_{AR} + X_{res} \quad (5.6)$$

5.7 EXPERIMENTAL RESULTS

Two sets of experiments were conducted to evaluate the reconstruction quality of the secret underwater image at the receiver end. Experiment 1 applied the SR based VSS (SRVSS) technique on the secret underwater image and computed the reconstruction quality of the secret underwater image using the HVS-based parameters. The experiment 2 have removed the various types of artifacts formed in experiment 1 using proposed CNN-based image enhancement architecture.

An open-source dataset of underwater images collected by Duarte *et al.* is used (Duarte et al. 2016) to test the presented model. The dataset consists of 84 images divided into three subsets. The first subset contains 20 images captured by adding milk turbidity. The second subset contains 20 images captured in a deep blue environment. The third subset, namely Chlorophyll, contains 20 front view images and 22 side-view images. The presented methodology was implemented using Matlab 2015a, running on Windows 10 Operating system with 16GB RAM.

5.7.1 Image quality Evaluation metrics

The reconstruction performance of the proposed technique was evaluated using popular HVS-based quality evaluation (Eskicioglu and Fisher (1995) parameters used in (Gujjuroori and Amberker (2013a,b); Mhala et al. (2018) like Self-similarity index (SSIM), Mean Square Error (MSE), Normalized Cross Correlation (NCC) and Normalized absolute error (NAE) respectively.

5.7.1.1 Self-similarity index (SSIM)

SSIM is the image quality metric, which evaluates the reconstruction quality of the SI in terms of luminance, contrast, and structural terms [Wang et al. \(2004\)](#). The simplified formula used to compute SSIM is given in Equation [5.7](#). Here \mathbf{I} represents original secret underwater image and \mathbf{R} represents reconstructed SI.

$$SSIM(I, R) = [l(I, R)]^\alpha \cdot [c(I, R)]^\beta \cdot [s(I, R)]^\gamma$$

Where,

$$l(I, R) = \frac{2\mu_I\mu_R + C1}{\mu_I^2 + \mu_R^2 + C2}, c(I, R) = \frac{2\sigma_I\sigma_R + C2}{\sigma_I^2 + \sigma_R^2 + C2}$$

$$s(I, R) = \frac{\sigma_{IR} + C3}{\sigma_I\sigma_R + C3}$$

where $\sigma_I, \sigma_R, \mu_I, \mu_R$, and σ_{IR} are the local standard deviations, means, and cross-covariance for images \mathbf{I} , \mathbf{R} . For $\alpha = \beta = \gamma = 1$ and $C3 = C2/2$, SSIM can be simplified as follows.

$$SSIM(I, R) = \frac{(2\mu_I\mu_R + C1)(2\sigma_{IR} + C2)}{(\mu_I^2 + \mu_R^2 + C1)(\sigma_I^2 + \sigma_R^2 + C2)} \quad (5.7)$$

5.7.1.2 Mean Square Error (MSE)

MSE computes the cumulative square error between two images. The formula shown in Equation [5.8](#) is used to compute MSE.

$$MSE^{HVS} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [\mathbf{I}(i, j) - \mathbf{R}(i, j)]^2 \quad (5.8)$$

Where \mathbf{I} denote the SI, and the \mathbf{R} denotes the reconstructed SI. The MSE provides values within range of zero and one. The value closer to zero indicates the better reconstruction quality of the SI.

5.7.1.3 Normalized Cross Correlation (NCC)

The normalized cross correlation provides the measure of similarity in terms of correlation between two images. The formula used for computation of NCC is given in Equation [5.9](#). The NCC ranges from zero to one, where one indicates that images are exactly similar, and zero indicates they are not similar to each other.

$$NCC = \frac{\sum_m \sum_n (I_{mn} - \bar{I})(R_{mn} - \bar{R})}{\sqrt{\left(\sum_m \sum_n (I_m - \bar{I})^2\right) \left(\sum_m \sum_n (R_{mn} - \bar{R})^2\right)}} \quad (5.9)$$

5.7.1.4 Normalized Absolute Error (NAE)

NAE is the measure of error between the original image and the reconstructed image. NAE of zero means the reconstructed image is of poor quality. Similarly, NAE being one indicates the better reconstruction quality of the SI. The formula used to compute the NAE is given in Equation 5.10.

$$NAE = \sum_{i=1}^m \sum_{j=1}^m \frac{\mathbf{I}(i, j) - \mathbf{R}(i, j)}{\mathbf{I}(i, j)} \quad (5.10)$$

5.7.2 Experiment 1: Performance evaluation of SR based VSS scheme

The first experiment have generated noise-like shares for each SI. The noise-like shares have a random noise-like appearance on the shares. The performance of the proposed technique was compared with the RVSS. The RVSS is a block-based VSS technique, which reconstructs the SI by embedding random pixels into shares to improve the reconstruction quality of the SI. The more details about the RVSS scheme can be found out in Chapter 3.

Table 5.6: The average values of HVS parameters for Chlorophyll (front view) images (The sample image is shown in Figure 5.7)

		MSE	NCC	NAE	SSIM
Experiment 1	RVSS Mhala et al. (2018)	1617.16	0.5815	0.2788	0.1761
	SRVSS Mhala and Pais (2019a)	50.8732	0.8443	0.0478	0.7499
Experiment 2	SRVSS after removal of artifact using ARCNN	35.3917	0.8805	0.0384	0.8101
	Proposed CNN-based SRVSS technique	30.7161	0.8874	0.0367	0.8296

The SSIM computed for the various underwater images is given in Tables 5.6, 5.7, 5.8, and 5.9 respectively. It is evident from Table 5.6 that VSS technique using SR reconstructs the SI with a better similarity index of 0.7499, whereas RVSS reconstructs the SI with a similarity index of 0.1761. Similarly, Tables 5.7, 5.8 and 5.9 show the same improved similarity index for the SRVSS technique than the RVSS scheme. The RVSS scheme has poor SSIM because it has embedded random pixel values in the middle frequency, which creates the blocking artifact effect in a reconstructed SI. The addition of

Table 5.7: The average values of HVS parameters for Chlorophyll (side view) images (The sample image is shown in Figure 5.9)

		MSE	NCC	NAE	SSIM
Experiment 1	RVSS Mhala et al. (2018)	1431.61	0.6692	0.2776	0.2750
	SRVSS Mhala and Pais (2019a)	49.1030	0.9799	0.0514	0.8269
Experiment 2	SRVSS after removal of artifact using ARCNN	33.4856	0.9867	0.0413	0.8740
	Proposed CNN-based SRVSS technique	26.7482	0.9888	0.0380	0.8967

Table 5.8: The average values of HVS parameters for Deep Blue images (The sample image is shown in Figure 5.10)

		MSE	NCC	NAE	SSIM
Experiment 1	RVSS Mhala et al. (2018)	988.68	0.3293	0.2675	0.7907
	SRVSS Mhala and Pais (2019a)	71.8412	0.5339	0.0925	0.9830
Experiment 2	SRVSS after removal of artifact using ARCNN	53.7614	0.6455	0.0699	0.9870
	Proposed CNN-based SRVSS technique	42.3158	0.6717	0.0648	0.9903

Table 5.9: The average values of HVS parameters for images with milk turbidity (The sample image is shown in Figure 5.11)

		MSE	NCC	NAE	SSIM
Experiment 1	RVSS Mhala et al. (2018)	1562.38	0.3500	0.2776	0.1354
	SRVSS Mhala and Pais (2019a)	48.6957	0.8444	0.0477	0.6940
Experiment 2	SRVSS after removal of artifact using ARCNN	33.1315	0.8805	0.0384	0.7693
	Proposed CNN-based SRVSS technique	29.3629	0.8874	0.0367	0.7889

blocking artifacts can be seen in Figures 5.7, 5.9, 5.10 and 5.11. Whereas this chapter embedded the LR pixel values instead of random pixels to avoid the blocking artifact formation in the middle locations. The use of the MISR technique ensures that the reconstructed image uses similar pixel values to enhance the visual quality of the SI.

The average MSE for the Chlorophyll (front view) images is 1617.16 for the RVSS

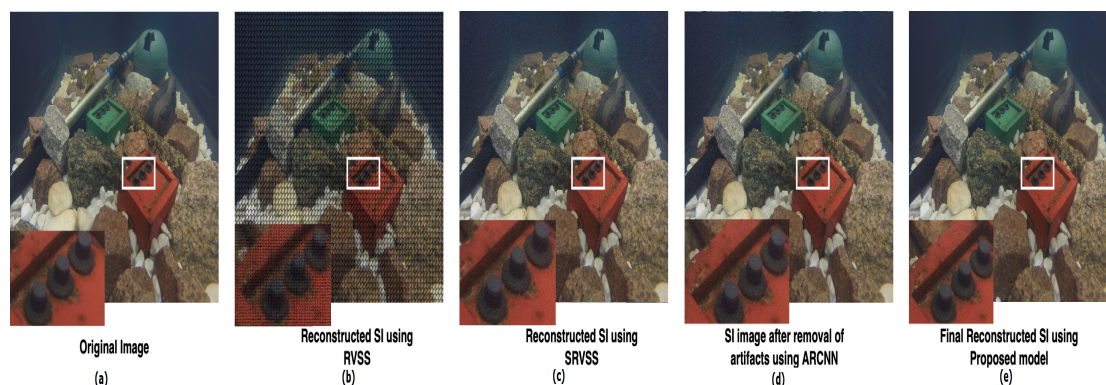


Figure 5.9: Reconstruction of secret Chlorophyll (Side view) underwater image. (a) The original underwater image, (b) Reconstructed underwater image using the RVSS scheme, (c) reconstructed underwater image using the SRVSS scheme, (d) the underwater image after removal of artifacts using ARCNN, and (e) final reconstructed underwater image using CNN-based VSS scheme. (The original image too large for display, hence the only part of an image is shown for better visualization)

images, whereas SRVSS reconstructs the SI with the less MSE of 50.8732. Similarly, for the remaining datasets, the average MSE is in the range of 48.6957 to 71.8412 for the SRVSS images and 988.68-1562.38 for the RVSS images.

Tables 5.6, 5.7, 5.8 and 5.9 show the average NCC between two images is in the range of 0.3293 - 0.6692 for the RVSS images, whereas the average NCC is better for the SRVSS (i.e. in the range of 0.5339 - 0.9799).

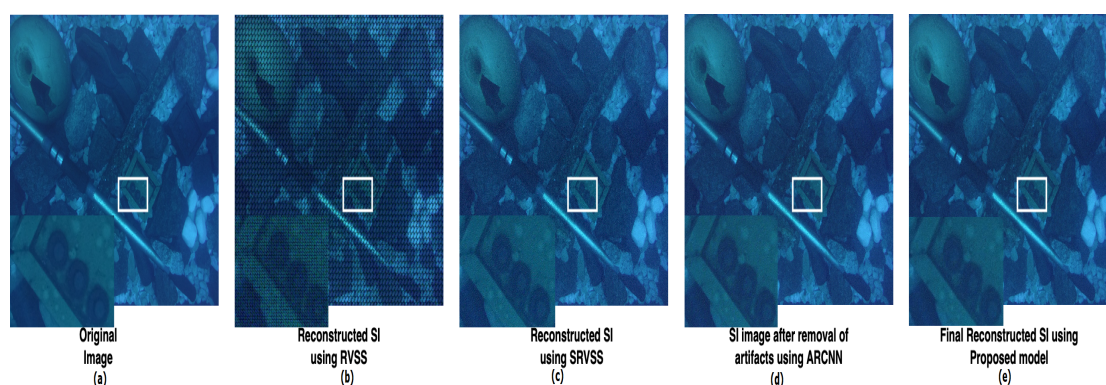


Figure 5.10: Reconstruction of secret Deep underwater image. (a) The original underwater image, (b) Reconstructed underwater image using the RVSS scheme, (c) reconstructed underwater image using the SRVSS scheme, (d) the underwater image after removal of artifacts using ARCNN, and (e) final reconstructed underwater image using CNN-based VSS scheme. (The original image too large for display, hence the only part of an image is shown for better visualization)

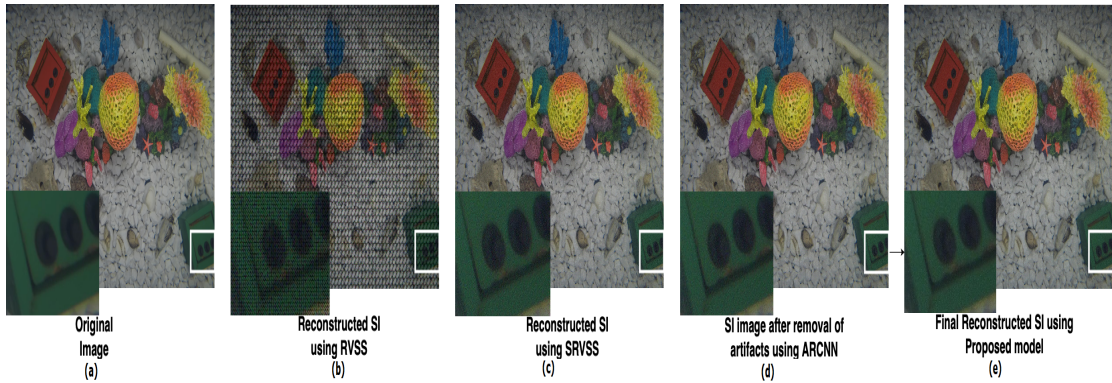


Figure 5.11: Reconstruction of the secret underwater image with added milk turbidity. (a) The original underwater image, (b) Reconstructed underwater image using the RVSS scheme, (c) reconstructed underwater image using the SRVSS scheme, (d) the underwater image after removal of artifacts using ARCNN, and (e) final reconstructed underwater image using CNN-based VSS scheme. (The original image too large for display, hence the only part of an image is shown for better visualization)

NAE for the given underwater dataset is in the range of 0.2775 - 0.2788 for the RVSS scheme. The NAE with SRVSS is in the range of 0.0478-0.0925 for the underwater images. It is evident from the given tables (5.6, 5.7, 5.8 and 5.9) that SRVSS outperforms the existing RVSS scheme in terms of HVS based parameters. Although SRVSS reconstructs SI with better visual similarity, it still leads to the addition of various types of artifacts. The experiment two evaluates the performance of the proposed a CNN-based model to reduce the various types of artifacts. The experimentation carried out to remove the artifact is discussed in the following subsection.

5.7.3 Experiment 2: Performance of the proposed system after applying CNN-based image enhancement architecture

In the second experiment presented scheme has removed the various artifacts present in reconstructed SI using the CNN-based model. The proposed method contains three steps, namely the initialization step, generation of residue image followed by the final output generation step. The proposed scheme adopted the ARCNN technique for the removal of ringing artifacts as a pre-processing step. The use of ARCNN technique in the first step ensures the formation of a better-initialized image to generate a better residue image. The learned initialized image using ARCNN is free from ringing artifacts and is smooth with less noise. The second step generates a residue image from the

initialized image. In the final step, the output is generated by adding the residue image to the artifact-free image.

Table 5.10: The network summary used by proposed system

Layer (type)	Output Shape	# Parameters
conv2d_1 (Conv2D)	(None, 24, 24, 64)	5248
conv2d_2 (Conv2D)	(None, 24, 24, 32)	100384
conv2d_3 (Conv2D)	(None, 24, 24, 16)	528
conv2d_4 (Conv2D)	(None, 20, 20, 1)	401
Total parameters :- 106,561		
Trainable parameters :- 106,561		
Non-trainable Parameters :- 0		

The first step have used the BSDS500 database (Martin et al. 2001) to train the model. The dataset contains the images collected from 30 human subjects. The dataset used in this proposed scheme has the property that it is useful for the detection of boundary and segmentation. Hence, proposed scheme used the BSDS500 dataset as a training dataset, which in turn provides a better reconstruction capability for underwater images. The ARCNN network is trained using 200 images and validated on 100 images. The training set is decomposed into images of size 32×32 . A total of 537,600 training images were used for this experiment. To avoid the border effect while reconstructing the original image, proposed scheme used a 20×20 size image as output. The summary of the ARCNN model used in this chapter is shown in Table 5.10. Table 5.10 shows the four convolution layers, that used a total 1,06,561 learning parameters to train the system. To test the performance of the system, the same underwater dataset as that of Experiment 1 were used. The underwater image dataset used in this scheme contains all types of images (i.e., with milk turbidity, deep water, and Chlorophyll).

The performance of the reconstructed images after removing the artifact is evaluated using MSE, NCC, NAE, and SSIM. From Table 5.6, it is evident that proposed scheme achieves better NCC and SSIM as compared to Experiment 1. It is also evident that the proposed technique contains less MSE and NAE error as compared to Experiment 1 techniques. Similarly, the better reconstruction quality in terms of HVS parameters for all the remaining databases (Tables 5.7, 5.8, 5.9) can also be observed. Figure 5.7

shows the SSIM computed for the underwater image from the Chlorophyll front view dataset. It is evident that the reconstructed image after removing the artifact is more smooth and is similar to the original underwater image. The images in the Chlorophyll (side view) database are recovered with a SSIM of 89.99% (Figure 5.9). Also, it can be observed that for the images that are uniform and have a more blue component (Figure 5.10) are reconstructed with almost 98.67% SSIM. The significant improvement in the reconstruction of deep underwater images is due to the presence of high-frequency information, that makes it more relevant to reconstruct. Whereas, for underwater images (Milk set), the proposed system reconstructs the SI with almost 81.39% SSIM (Figure 5.11).

The second step used the same BSDS500 database to train the network. The patches of size 64×64 were extracted from the training images. Before the extraction of training patches, proposed scheme have generated compressed images using standard JPEG compression scheme with the quality (q) settings of $q= 10, 20, 30$ and 40 (from very low to high quality) to learn about the various artifacts. A MATLAB JPEG encoder is used to generate these different quality images.

The residual labels for the deep CNN model were generated using the equation given in 5.11. Where X_{res} denotes the residual image, X represents the original image from the train set, and X_{in} represents the compressed image given as input to the deep CNN model as a training image.

$$X_{res} = X - X_{in} \quad (5.11)$$

The presented test set have generated the residual image and added it to the artifact-free image to get the final output. The CNN architecture used in this scheme is shown layer by layer in Table 5.11 in detail. A total of 16 blocks were used in this scheme, as defined in the previous subsection 5.6.2. The Proposed network is trained for 30 iterations. The proposed scheme have trained system on 70% images and validated using 30% images. For testing the model, proposed scheme have used the same test dataset of underwater images considered in Experiment 1. The quality of the final images is evaluated using the HVS-based parameters. The MSE, NCC, NAE, and SSIM of the final output is compared with the original image to evaluate the performance of the sys-

tem. The average results for Chlorophyll (front view) underwater images are shown in Table 5.6. The improved quality of the image with better HVS parameters is evident from Table 5.6. Similarly, the average results of the underwater images with Chlorophyll (side view), Deep Blue, and added milk turbidity are shown in Tables 5.7, 5.8 and 5.9 respectively. The sample images from each underwater dataset is shown in Figures 5.7, 5.9, 5.10 and 5.11. From Figures 5.7, 5.9, 5.10 and 5.11, it is evident that final reconstructed image contains SSIM of 85.73%, 91.94%, 98.97% and 82.80% for the sample Chlorophyll (front view), Chlorophyll (side view), Deep underwater and Milk turbid database image. The final reconstructed image contains a clear, sharp image along the edges. The addition of the residue image into the initialized image, acted as a cue to sharpen the SI.

Table 5.11: The details of each layer used in a deep CNN network to predict the residual image

Block	CR	CBR						
Layer	CR	CBR1	CBR2	CBR3	CBR3	CBR5	CBR6	CBR7
Kernel Size	3×3	3×3	3×3	3×3	3×3	3×3	3×3	3×3
Filter size	64	64	64	64	64	64	64	64
Padding	same	same	same	same	same	same	same	same
Stride	1	1	1	1	1	1	1	1
Block	CBR							C
Layer	CBR8	CBR9	CBR10	CBR11	CBR12	CBR13	CBR14	C
Kernel Size	3×3	3×3	3×3	3×3	3×3	3×3	3×3	3×3
Filter size	64	64	64	64	64	64	64	3
Padding	same	same	same	same	same	same	same	same
Stride	1	1	1	1	1	1	1	1

The presented system also have an advantage that it encrypts the SI shares using DCT, which makes the proposed system more secure. Even though the adversary gets hold of transmitted shares, he can't get back the SI. In order to recover the entire SI, the adversary must have all shares. Also, if the adversary performs the inverse DCT on transmitted shares, he will still get an encrypted share, which is of no use unless the adversary has all the shares. Hence generation of doubly encrypted shares makes it even harder for an adversary to get back the SI.

5.8 SUMMARY

This chapter presented a VSS based applications for medical images and the underwater images. Firstly, this chapter have applied a technique presented in Chapter 4 for contrast enhancement in case of PVSS schemes using SR on the medical image. The scheme uses the reversible data hiding technique to improve the contrast of recovered medical image. A MAP-BTV approach is used to minimize the cost function for the SR problem. The proposed scheme recovers medical images with the contrast of 70-80% for meaningful shares and 99% for noise-like shares. Scheme also recovers medical image without any blocking artifact. Hence provides the visually better smooth image which is free from blocking artifacts. Additionally, the experiment were carried out with popularly used CAD system to demonstrate the efficiency of the VSS technique on medical images.

The underwater images contain important information about the minerals, metals, etc. which needs to be communicated over a network. This chapter has presented a secure VSS scheme for underwater images. The technique used SRVSS technique presented in Chapter 4 to transmit images over a network. The experimental results showed that the SR-based VSS scheme could recover the SI with a better SSIM of almost 78-98%. Although the SR-based VSS scheme reconstructs the SI with better visual quality, it still suffers from various types of artifacts. In order to remove these artifacts, this chapter also proposed a novel CNN-based architecture that uses a residual image to improve the visual quality of the SI. The experimental results show that the CNN-based architecture achieves a better visual similarity of almost 86-99% SSIM for the SI as compared to existing block based VSS schemes.

CHAPTER 6

CONCLUSIONS AND FUTURE SCOPE

Visual Secret Sharing (VSS) is a technique that secures visual information by concealing the original visual information in the form of multiple shares. It is a very useful technique as decryption can be done using Human Visual System. This thesis has presented the literature survey of many visual cryptography techniques. The methods discussed in the thesis suffer from common drawbacks like an expansion of recovered image, restriction on a number of users, recovery of multi-tone image as a binary image, etc. The block-based Visual Secret Sharing (BPVSS) scheme is a VSS scheme, which tries to solve the many drawbacks. But still, it suffers from common problems like i) The existing BPVSS technique provides the contrast of at-most 50% for gray-level images and 25% for color images, and ii) BPVSS recovers the monotone image as output for multi-tone images. To solve the poor contrast problem, this thesis proposed multiple techniques.

Firstly, Chapter 3 presented an RVSS method, which is an effective method for securely sharing visual information. The proposed scheme has the following advantages as compared to the BPVSS scheme.

- The presented scheme recovers the image with the contrast of 70-90% and 70-80% for noise-like shares and meaningful shares, respectively.
- The presented scheme recovers the image in a similar format (i.e., grey-scale or color) as the secret image.

The RVSS scheme method restores the secret image with good contrast and quality without any leakage of information from any shares. The RVSS scheme produces blocking artifacts because of the position of data embedding. The blocking artifact appears in the middle of each block because the RVSS scheme has used the middle position to embed the data. The scheme proposed in Chapter 3 achieved the first objective of the thesis. To solve the problem of blocking artifacts, Chapter 4 proposed a novel Super-resolution based Visual Secret Sharing (SRVSS) scheme.

The SRVSS scheme presented in Chapter 4 used a reversible data hiding technique to improve the contrast of the recovered image. The SRVSS scheme has embedded low-resolution images into shares. Further, the SRVSS scheme used hidden low-resolution images to improve the contrast of the secret image and also reduce blocking artifacts. The SRVSS scheme used a super-resolution technique at the receiver end to improve the visual quality of the secret image. A MAP-BTV approach is used to minimize the cost function for the proposed problem. The SRVSS scheme recovers secret images with the contrast of 70-80% for meaningful shares and 99% for noise-like shares. The advantage of the SRVSS scheme over the RVSS scheme is that it recovers images without any blocking artifact. The proposed scheme provides a visually better smooth image, which is free from blocking artifacts. The technique proposed in Chapter 4 achieves the second objective of the thesis.

Chapter 5 has presented two VSS-based applications. The first application used the concept of super-resolution to improve the contrast of a secret medical image. This scheme hides the low-resolution image information about the secret medical image into shares. Further, hidden pixel information is used to improve the quality of the reconstructed image. From Chapter 3, it is evident that the RVSS scheme suffers from a problem of the artifact while recovering the secret image. Whereas experimental results carried out in Chapter 5 showed that recovered secret medical image using the SRVSS scheme is free from blocking artifacts. Also, the recovered secret image can be used for CAD.

The second application is presented for underwater images. The underwater image contains essential information that needs to be communicated securely over a network.

Visual Secret Sharing (VSS) is a modern cryptography technique, which conceals the secret image into multiple shares, and these shares are then transmitted over a network to participants. Once the participant receives the shares, they need to stack them together to recover the secret underwater image. Chapter 5 proposed an SR-based VSS scheme, which recovers the SI using multiple LR images. The experimental results showed that the SR-based VSS scheme could recover the SI with a better SSIM of almost 78-98%. Although the SR-based VSS scheme reconstructs the SI with better visual quality, it still suffers from various types of artifacts. In order to remove these artifacts, in this thesis, a novel CNN-based architecture was proposed, which uses a residual image to improve the visual quality of the secret image. The experimental results showed that the CNN-based architecture achieves a better visual similarity of almost 86-99% SSIM for the secret image as compared to existing block-based VSS schemes. The experiment also showed that the proposed CNN-based scheme outperforms the existing RVSS and SRVSS schemes in terms of HVS-based parameters to recover the SI. Chapter 5 has achieved the third objective defined in this thesis by proposing a CNN-based VSS scheme for underwater images.

Future Scope

In future, contrast of the various techniques proposed in this thesis can be improved by experimenting with different types of Super-resolution techniques. Also, a preliminary experiment conducted to remove artifacts using the CNN-based technique (Chapter 5) showed better improvement in the quality of the SI. Further, a better artifact removal techniques by adding more layers and tuning the hyper-parameters of CNN architecture can be explored. Often underwater images contain the turbidity. So adding turbidity removal step as a pre-processing step can further improve the quality of the recovered underwater images.

BIBLIOGRAPHY

- (2015) ftp://ftp.cs.technion.ac.il/pub/projects/medic-image/breast_cancer_data/). accessed on 19-July-2016.
- Ateniese, G., Blundo, C., De Santis, A. and Stinson, D. R. (1996). “Visual cryptography for general access structures.” *Information and Computation*, 129(2), 86–106.
- Ateniese, G., Blundo, C., De Santis, A. and Stinson, D. R. (2001). “Extended capabilities for visual cryptography.” *Theoretical Computer Science*, 250(1), 143–161.
- Bertsekas, D. P. (1999). *Nonlinear programming*, Athena scientific Belmont.
- Bhandari, S. H. (2015). “A bag-of-features approach for malignancy detection in breast histopathology images.” In *Image Processing (ICIP), 2015 IEEE International Conference on*, IEEE, 4932–4936.
- Blundo, C., De Santis, A. and Naor, M. (2000). “Visual cryptography for grey level images.” *Information Processing Letters*, 75(6), 255–259.
- Chang, C.-C., Chen, T.-S. and Chung, L.-Z. (2002). “A steganographic method based upon jpeg and quantization table modification.” *Information Sciences*, 141(1), 123–138.
- Chang, C.-C., Lin, C.-C., Tseng, C.-S. and Tai, W.-L. (2007). “Reversible hiding in dct-based compressed images.” *Information Sciences*, 177(13), 2768–2786.
- Chen, S.-K. (2009a). “Friendly progressive visual secret sharing using generalized random grids.” *Optical Engineering*, 48(11), 117001–1.

- Chen, S.-K. (2009b). “Friendly progressive visual secret sharing using generalized random grids.” *Optical Engineering*, 48(11), 117001–1.
- Cheng, Y., Fu, Z. and Yu, B. (2018). “Improved visual secret sharing scheme for qr code applications.” *IEEE Transactions on Information Forensics and Security*, 13(9), 2393–2403.
- Chin, C. S., Jin, A. T. B. and Ling, D. N. C. (2006). “High security iris verification system based on random secret integration.” *Computer Vision and Image Understanding*, 102(2), 169–177.
- Chung, K.-L. and Wu, S.-T. (2005). “Inverse halftoning algorithm using edge-based lookup table approach.” *IEEE Transactions on Image Processing*, 14(10), 1583–1589.
- Cruz-Roa, A., Caicedo, J. C. and González, F. A. (2011). “Visual pattern mining in histology image collections using bag of features.” *Artificial intelligence in medicine*, 52(2), 91–106.
- Csurka, G., Dance, C., Fan, L., Willamowski, J. and Bray, C. (2004). “Visual categorization with bags of keypoints.” In *Workshop on statistical learning in computer vision, ECCV*, volume 1, Prague, 1–2.
- Dian, R., Li, S., Guo, A. and Fang, L. (2018). “Deep hyperspectral image sharpening.” *IEEE transactions on neural networks and learning systems*, (99), 1–11.
- Divya, C. and Surya, E. (2012). “Visual cryptography using palm print based on dct algorithm.” *International Journal of Emerging Technology and Advanced Engineering*, 2(12), 2250–2459.
- Dong, C., Deng, Y., Change Loy, C. and Tang, X. (2015). “Compression artifacts reduction by a deep convolutional network.” In *Proceedings of the IEEE International Conference on Computer Vision*, 576–584.

- Dong, C., Loy, C. C., He, K. and Tang, X. (2016). “Image super-resolution using deep convolutional networks.” *IEEE transactions on pattern analysis and machine intelligence*, 38(2), 295–307.
- Duarte, A., Codevilla, F., Gaya, J. D. O. and Botelho, S. S. (2016). “A dataset to evaluate underwater image restoration methods.” In *OCEANS 2016-Shanghai*, IEEE, 1–6.
- Elad, M. and Feuer, A. (1997). “Restoration of a single superresolution image from several blurred, noisy, and undersampled measured images.” *IEEE transactions on image processing*, 6(12), 1646–1658.
- Eskicioglu, A. M. and Fisher, P. S. (1995). “Image quality measures and their performance.” *IEEE Transactions on communications*, 43(12), 2959–2965.
- Fadnavis, S. (2014). “Image interpolation techniques in digital image processing: an overview.” *International Journal of Engineering Research and Applications*, 4(10), 70–73.
- Fan, D.-P., Lin, Z., Zhang, Z., Zhu, M. and Cheng, M.-M. (2020). “Rethinking rgb-d salient object detection: Models, data sets, and large-scale benchmarks.” *IEEE Transactions on Neural Networks and Learning Systems*.
- Fang, W.-P. (2008a). “Friendly progressive visual secret sharing.” *Pattern Recognition*, 41(4), 1410–1414.
- Fang, W.-P. (2008b). “Friendly progressive visual secret sharing.” *Pattern Recognition*, 41(4), 1410–1414.
- Fang, W.-P. and Lin, J.-C. (2006a). “Progressive viewing and sharing of sensitive images.” *Pattern recognition and Image analysis*, 16(4), 632–636.
- Fang, W.-P. and Lin, J.-C. (2006b). “Progressive viewing and sharing of sensitive images.” *Pattern recognition and Image analysis*, 16(4), 632–636.
- Farsiu, S., Robinson, M. D., Elad, M. and Milanfar, P. (2004). “Fast and robust multi-frame super resolution.” *IEEE transactions on image processing*, 13(10), 1327–1344.

BIBLIOGRAPHY

- Floyd, R. W. (1976). “An adaptive algorithm for spatial gray-scale.” In *Proc. Soc. Inf. Disp.*, volume 17, 75–77.
- Fu, K., Fan, D.-P., Ji, G.-P. and Zhao, Q. (2020). “Jl-dcf: Joint learning and densely-cooperative fusion framework for rgb-d salient object detection.” In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 3052–3062.
- Fu, K., Zhao, Q., Gu, I. Y.-H. and Yang, J. (2019). “Deepside: A general deep framework for salient object detection.” *Neurocomputing*, 356, 69–82.
- Glasby, G. (2000). “Lessons learned from deep-sea mining.” *Science*, 289(5479), 551–553.
- Gonzalez, R. and Wintz, P. (1977). “Digital image processing.” .
- Gujjunoori, S. and Amberker, B. (2013a). “Busyembed: an hvs based reversible data embedding scheme for video using dct.” .
- Gujjunoori, S. and Amberker, B. (2013b). “Dct based reversible data embedding for mpeg-4 video using hvs characteristics.” *Journal of information security and applications*, 18(4), 157–166.
- Halfar, J. and Fujita, R. M. (2007). “Danger of deep-sea mining.” *Science*, 316(5827), 987–987.
- He, H. and Kondi, L. P. (2006). “An image super-resolution algorithm for different error levels per frame.” *IEEE Transactions on Image Processing*, 15(3), 592–603.
- He, K., Zhang, X., Ren, S. and Sun, J. (2016). “Deep residual learning for image recognition.” In *Proceedings of the IEEE conference on computer vision and pattern recognition*, 770–778.
- Hou, Y.-C. (2003). “Visual cryptography for color images.” *Pattern recognition*, 36(7), 1619–1629.
- Hou, Y. C. (2012). “BPVSS.” <http://mail.im.tku.edu.tw/~ychou/BPVSS/>. [Online; accessed 21-Oct-2016].

- Hou, Y.-C. and Quan, Z.-Y. (2011a). “Progressive visual cryptography with unexpanded shares.” *IEEE Transactions on Circuits and Systems for Video Technology*, 21(11), 1760–1764.
- Hou, Y.-C. and Quan, Z.-Y. (2011b). “Progressive visual cryptography with unexpanded shares.” *IEEE Transactions on Circuits and Systems for Video Technology*, 21(11), 1760–1764.
- Hou, Y.-C., Quan, Z.-Y., Tsai, C.-F. and Tseng, A.-Y. (2013a). “Block-based progressive visual secret sharing.” *Information Sciences*, 233, 290–304.
- Hou, Y.-C., Quan, Z.-Y., Tsai, C.-F. and Tseng, A.-Y. (2013b). “Block-based progressive visual secret sharing.” *Information Sciences*, 233, 290–304.
- Hou, Y.-C., Wei, S.-C., Lin, C.-Y., Wei, S.-C. et al. (2014). “Random-grid-based visual cryptography schemes.” *IEEE Transactions on Circuits and Systems for Video Technology* 24 (5), 733–744.
- Irani, M. and Peleg, S. (1991). “Improving resolution by image registration.” *CVGIP: Graphical models and image processing*, 53(3), 231–239.
- Irani, M. and Peleg, S. (1993). “Motion analysis for image enhancement: Resolution, occlusion, and transparency.” *Journal of Visual Communication and Image Representation*, 4(4), 324–335.
- Ito, R., Kuwakado, H. and Tanaka, H. (1999). “Image size invariant visual cryptography.” *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 82(10), 2172–2177.
- Iwamoto, M. and Yamamoto, H. (2002). “The optimal n-out-of-n visual secret sharing scheme for gray-scale images.” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 85(10), 2238–2247.
- Iwata, M., Miyake, K. and Shiozaki, A. (2004). “Digital steganography utilizing features of jpeg images.” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 87(4), 929–936.

- Jain, A. K. (1989). *Fundamentals of digital image processing*, Prentice-Hall, Inc.
- Joshi, M. V., Chaudhuri, S. and Panuganti, R. (2005). “A learning-based method for image super-resolution from zoomed observations.” *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 35(3), 527–537.
- Kaur, H. and Khanna, P. (2016). “Biometric template protection using cancelable biometrics and visual cryptography techniques.” *Multimedia Tools and Applications*, 75(23), 16333–16361.
- Kite, T. D., Damera-Venkata, N., Evans, B. L. and Bovik, A. C. (2000). “A fast, high-quality inverse halftoning algorithm for error diffused halftones.” *IEEE Transactions on Image Processing*, 9(9), 1583–1592.
- Kumar, N. et al. (2020). “On generating cancelable biometric templates using visual secret sharing.” In *Science and Information Conference*, Springer, 532–544.
- Lee, E. S. and Kang, M. G. (2003). “Regularized adaptive high-resolution image reconstruction considering inaccurate subpixel registration.” *IEEE Transactions on Image Processing*, 12(7), 826–837.
- Lin, C.-C. and Tsai, W.-H. (2003). “Visual cryptography for gray-level images by dithering techniques.” *Pattern Recognition Letters*, 24(1), 349–358.
- Lowe, D. G. (2004). “Distinctive image features from scale-invariant keypoints.” *International journal of computer vision*, 60(2), 91–110.
- MacPherson, L. (2002). “Grey level visual cryptography for general access structures.” Master’s thesis, University of Waterloo.
- Martin, D., Fowlkes, C., Tal, D. and Malik, J. (2001). “A database of human segmented natural images and its application to evaluating segmentation algorithms and measuring ecological statistics.” In *Proceedings Eighth IEEE International Conference on Computer Vision. ICCV 2001*, volume 2, IEEE, 416–423.
- Mese, M. and Vaidyanathan, P. P. (2001). “Look-up table (lut) method for inverse halftoning.” *IEEE Transactions on Image Processing*, 10(10), 1566–1578.

- Mhala, N. C. and Bhandari, S. H. (2016). “Improved approach towards classification of histopathology images using bag-of-features.” In *Signal and Information Processing (ICONSIP), International Conference on*, IEEE, 1–5.
- Mhala, N. C., Jamal, R. and Pais, A. R. (2018). “Randomised visual secret sharing scheme for grey-scale and colour images.” *IET Image Processing*, 12, 422–431(9).
- Mhala, N. C. and Pais, A. R. (2019a). “Contrast enhancement of progressive visual secret sharing (pvss) scheme for gray-scale and color images using super-resolution.” *Signal Processing*, 162, 253–267.
- Mhala, N. C. and Pais, A. R. (2019b). “An improved and secure visual secret sharing (vss) scheme for medical images.” In *2019 11th International Conference on Communication Systems & Networks (COMSNETS)*, IEEE, 823–828.
- Mhala, N. C. and Pais, A. R. (2020). “A secure visual secret sharing (vss) scheme with cnn-based image enhancement for underwater images.” *The Visual Computer*, 1–15.
- Monoth, T. et al. (2010). “Tamperproof transmission of fingerprints using visual cryptography schemes.” *Procedia Computer Science*, 2, 143–148.
- Naor, M. and Shamir, A. (1994a). “Visual cryptography.” In *Workshop on the Theory and Application of Cryptographic Techniques*, Springer, 1–12.
- Naor, M. and Shamir, A. (1994b). “Visual cryptography.” In *Workshop on the Theory and Application of Cryptographic Techniques*, Springer, 1–12.
- Nasrollahi, K. and Moeslund, T. B. (2014). “Super-resolution: a comprehensive survey.” *Machine vision and applications*, 25(6), 1423–1468.
- Ng, M. K., Shen, H., Lam, E. Y. and Zhang, L. (2007). “A total variation regularization based super-resolution reconstruction algorithm for digital video.” *EURASIP Journal on Advances in Signal Processing*, 2007(1), 074585.
- Nocedal, J. and Wright, S. J. (2006). “Numerical optimization 2nd.”).

BIBLIOGRAPHY

- of Southern California, U. U. (1977). “USC-SIPI.” <http://sipi.usc.edu/database/database.php?volume=misc?>). [Online; accessed 19-Nov-2016].
- Ogawa, Y., Ariki, Y. and Takiguchi, T. (2012). “Super-resolution by gmm based conversion using self-reduction image.” In *Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference on*, IEEE, 1285–1288.
- Park, M. K., Kang, M.-G. and Katsaggelos, A. K. (2007). “Regularized high-resolution image reconstruction considering inaccurate motion information.” *Optical Engineering*, 46(11), 117004.
- Patanavijit, V. and Jitapunkul, S. (2006). “A robust iterative multiframe super-resolution reconstruction using a huber bayesian approach with huber-tikhonov regularization.” In *Intelligent Signal Processing and Communications, 2006. ISPACS’06. International Symposium on*, IEEE, 13–16.
- Patanavijit, V. and Jitapunkul, S. (2007). “A lorentzian stochastic estimation for a robust iterative multiframe super-resolution reconstruction with lorentzian-tikhonov regularization.” *EURASIP Journal on Advances in Signal Processing*, 2007(2), 21–21.
- Rajan, D. and Chaudhuri, S. (2001). “Generation of super-resolution images from blurred observations using markov random fields.” In *Acoustics, Speech, and Signal Processing, 2001. Proceedings.(ICASSP’01). 2001 IEEE International Conference on*, volume 3, IEEE, 1837–1840.
- Revenkar, P., Anjum, A. and Gandhare, W. (2010). “Secure iris authentication using visual cryptography.” *arXiv preprint arXiv:1004.1748*.
- Rijmen, V. (1996). “Efficient colour visual encryption or ‘shared colors of beneton’.” *Rump session of Eurocrypt’96*.
- Rohit, U., George, S. N. et al. (2017). “A robust face hallucination technique based on adaptive learning method.” *Multimedia Tools and Applications*, 76(15), 16809–16829.

- Ross, A. and Othman, A. A. (2010). “Visual cryptography for face privacy.” In *Biometric Technology for Human Identification VII*, volume 7667, International Society for Optics and Photonics, 76670B.
- Rudin, L. I., Osher, S. and Fatemi, E. (1992). “Nonlinear total variation based noise removal algorithms.” *Physica D: nonlinear phenomena*, 60(1-4), 259–268.
- Sinduja, R., Sathiya, R. and Vaithiyathan, V. (2012). “Sheltered iris attestation by means of visual cryptography (sia-vc).” In *IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM-2012)*, IEEE, 650–655.
- Smith, P. (1981). “Bilinear interpolation of digital images.” *Ultramicroscopy*, 6(2), 201–204.
- Sun, J., Xu, Z. and Shum, H.-Y. (2008). “Image super-resolution using gradient profile prior.” In *Computer Vision and Pattern Recognition, 2008. CVPR 2008. IEEE Conference on*, IEEE, 1–8.
- Sun, J., Xu, Z. and Shum, H.-Y. (2011). “Gradient profile prior and its applications in image super-resolution and enhancement.” *IEEE Transactions on Image Processing*, 20(6), 1529–1542.
- Timofte, R., De Smet, V. and Van Gool, L. (2013). “Anchored neighborhood regression for fast example-based super-resolution.” In *Proceedings of the IEEE international conference on computer vision*, 1920–1927.
- Timofte, R., De Smet, V. and Van Gool, L. (2014). “A+: Adjusted anchored neighborhood regression for fast super-resolution.” In *Asian conference on computer vision*, Springer, 111–126.
- Tsai, R. (1984). “Multiframe image restoration and registration.” *Adv. Comput. Vis. Image Process.*, 1(2), 317–339.
- Ulichney, R. (1999). “The void-and-cluster method for dither array generation.” *SPIE MILESTONE SERIES MS*, 154, 183–194.

- Wang, R.-Z. (2009a). “Region incrementing visual cryptography.” *IEEE Signal Processing Letters*, 16(8), 659–662.
- Wang, R.-Z. (2009b). “Region incrementing visual cryptography.” *IEEE Signal Processing Letters*, 16(8), 659–662.
- Wang, R.-Z., Lee, Y.-K., Huang, S.-Y. and Chia, T.-L. (2007a). “Multilevel visual secret sharing.” In *Innovative Computing, Information and Control, 2007. ICICIC’07. Second International Conference on*, IEEE, 283–283.
- Wang, R.-Z., Lee, Y.-K., Huang, S.-Y. and Chia, T.-L. (2007b). “Multilevel visual secret sharing.” In *Innovative Computing, Information and Control, 2007. ICICIC’07. Second International Conference on*, IEEE, 283–283.
- Wang, Z., Arce, G. R. and Di Crescenzo, G. (2009). “Halftone visual cryptography via error diffusion.” *IEEE transactions on information forensics and security*, 4(3), 383–396.
- Wang, Z., Bovik, A. C., Sheikh, H. R. and Simoncelli, E. P. (2004). “Image quality assessment: from error visibility to structural similarity.” *IEEE transactions on image processing*, 13(4), 600–612.
- Xiong, Zixiang Orchard, M. T. R. K. (1999). “Inverse halftoning using wavelets.” *IEEE transactions on image processing*, 8(10), 1479–1483.
- Yang, C.-N. and Chen, T.-S. (2005). “Extended visual secret sharing schemes with high-quality shadow images using gray sub pixels.” In *International Conference Image Analysis and Recognition*, Springer, 1184–1191.
- Yang, J., Wang, Z., Lin, Z., Cohen, S. and Huang, T. (2012a). “Coupled dictionary training for image super-resolution.” *IEEE transactions on image processing*, 21(8), 3467–3478.
- Yang, J., Wright, J., Huang, T. S. and Ma, Y. (2010). “Image super-resolution via sparse representation.” *IEEE transactions on image processing*, 19(11), 2861–2873.

- Yang, M.-C., Huang, D.-A., Tsai, C.-Y. and Wang, Y.-C. F. (2012b). “Self-learning of edge-preserving single image super-resolution via contourlet transform.” In *Multimedia and Expo (ICME), 2012 IEEE International Conference on*, IEEE, 574–579.
- Zeyde, R., Elad, M. and Protter, M. (2010). “On single image scale-up using sparse-representations.” In *International conference on curves and surfaces*, Springer, 711–730.
- Zhang, K., Zuo, W., Chen, Y., Meng, D. and Zhang, L. (2017). “Beyond a gaussian denoiser: Residual learning of deep cnn for image denoising.” *IEEE Transactions on Image Processing*, 26(7), 3142–3155.
- Zhao, J.-X., Liu, J.-J., Fan, D.-P., Cao, Y., Yang, J. and Cheng, M.-M. (2019). “Egnet: Edge guidance network for salient object detection.” In *Proceedings of the IEEE International Conference on Computer Vision*, 8779–8788.
- Zheng, W., Wang, K. and Wang, F.-Y. (2020). “Gan-based key secret-sharing scheme in blockchain.” *IEEE transactions on cybernetics*, 51(1), 393–404.
- Zhou, Z., Arce, G. R. and Di Crescenzo, G. (2006a). “Halftone visual cryptography.” *IEEE transactions on image processing*, 15(8), 2441–2453.
- Zhou, Z., Arce, G. R. and Di Crescenzo, G. (2006b). “Halftone visual cryptography.” *IEEE transactions on image processing*, 15(8), 2441–2453.

RESEARCH OUTCOMES

PUBLICATIONS

1. Mhala N. C., Jamal, R., and Pais A. R. (2018). Randomised visual secret sharing scheme for gray-scale and colour images. *IET Image Processing (IET)*, 12:422-431 (9). [DOI: <https://doi.org/10.1049/iet-ipr.2017.0759>]
2. Mhala N. C. and Pais A. R. (2019). Contrast enhancement of progressive visual secret sharing (PVSS) scheme for gray-scale and color images using super-resolution. *Signal Processing (Elsevier)*, 162:253-267. [DOI: <https://doi.org/10.1016/j.sigpro.2019.04.023>]
3. Mhala N. C. and Pais, A. R. (2020). A Secure Visual Secret Sharing (VSS) Scheme with CNN-based image enhancement for underwater images. *The Visual Computer (Springer)* [DOI: <https://doi.org/10.1007/s00371-020-01972-9>]
4. Mhala N. C. and Pais, A. R. (2019). An improved and secure visual secret sharing (vss) scheme for medical images. *In 2019 11th International Conference on Communication Systems & Networks (COMSNETS), pages 823–828. IEEE* [DOI: <https://doi.org/10.1109/COMSNETS.2019.8711327>]
5. Srujana, O. S., Mhala, N. C., and Pais, A. R (2020). Secure transmission of hyperspectral images. *In 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP), pages 94–99. IEEE* [DOI: <https://doi.org/10.1109/ISEA-ISAP49340.2020.235006>]

BIO-DATA

Name: Nikhil Chandrakant Mhala
Date of Birth: 25/11/1991
Gender: Male
Marital Status: Single
Father's Name: Chandrakant Mhala
Mother's Name: Chaya
Email Id: mhala.nikhil@gmail.com
Present Address: At Po. Asadpur Ta. Achalpur Dist Amravati
444806 (Maharashtra)
Educational Qualifications: B.E. (CSE) - PRCEAM, Badnera Amravati
(Maharashtra)
M.Tech (CSE) - Walchand College of Engg.
Sangli (Maharashtra)
Areas of Interest: Visual Cryptography, Image Security, Infor-
mation Security, Image Processing.
Email ID: mhala[DOT]nikhil[AT]gmail[DOT]com
Mobile No: (+91) 7588751166