Extended Visual Cryptography Techniques for True Color Images

Dissertation

submitted in partial fulfillment of the requirements

for the award of degree of

Master of Engineering in Software Engineering

Submitted By

Kirti Dhiman
(801531007)

Under the Supervision of

Dr. Singara Singh Kasana
Assistant Professor

Ms. Harkiran Kaur
Lecturer

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

JULY 2017

Certificate

I hereby certify that the work which is being presented in the thesis entitled, *"Extended Visual Cryptography Techniques for True Color Images"*, in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Software Engineering* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Singara Singh Kasana* and *Ms. Harkiran Kaur*.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Kirti Dhiman

(Kirti Dhiman)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Singara Singh Kasana)
Assistant Professor
CSED
Thapar University
Patiala

(Ms. Harkiran Kaur)
Lecturer
CSED
Thapar University
Patiala

Acknowledgment

I have been waiting long for this moment to acknowledge all those who contributed in building this work. It is my pleasure to thank all of them here. First of all, I offer my sincere gratitude to my supervisors, *Dr. Singara Singh Kasana* and *Ms. Harkiran Kaur*, for accepting to be my supervisors. Without their help and encouraging advice, this work would have never begun. I am deeply indebted to them for providing me wonderful research atmosphere and platform to explore my research to the fullest.

I am also grateful to *Dr. Maninder Singh*, Head, CSED for providing me the opportunity to conduct my research work. I would also like to thank the Director of the institute, *Prof. Prakash Gopalan* for his continuous support.

My special thanks goes to my friends for discussing thoughts and sharing all ups and downs with me during the course of this work. At the same time I would also like to thank all my colleagues for their continuous support.

Last but not the least I would like to thank my parents and family members, who made me capable of reaching this point of life and for giving me their kind support and love. I dedicate my work to them.

Kirti Dhiman.

Kirti Dhiman

(801531007)

Abstract

In the digital era, Internet is the basic necessity for exchanging any multimedia data over the widespread network. As long as the communication network is untrusted, data security and privacy plays a major role. Images are important form of multimedia data which are excessively transferred over the Internet. Various techniques and algorithms have been proposed by researchers to securely transmit the images over the network while performing very less computations during encryption/decryption. Visual Cryptography provides basic and convenient way to share the secret and confidential images with ease.

Various Visual Cryptography Techniques and Extended Visual Cryptography Techniques for binary, gray-scale and colored images have been proposed by researchers to improve the security and contrast of the reconstructed image. Two new (k, n)-EVCTs for true color images are proposed in this thesis work. First technique is (3, 3)-EVCT and second one is (2, 3)-EVCT. Both techniques share a single secret true RGB color image at a time.

In (3, 3)-EVCT, three meaningful shares are generated *i.e.*, R share, G share and B share. 3-out-of-3 shares are required to regenerate the original secret image on the receiver side. Less than three shares would not be able to regenerate the original secret image. In (2, 3)-EVCT, generated shares are RG share, GB share and RB share. At least any 2-out-of-3 shares are required to regenerate the original secret image. Both techniques are efficient, simple and convenient to use. The reconstruct image generates without any loss in image size, contrast, resolution and visual quality. The techniques are also compared with various existing techniques to show their effectiveness.

Contents

List of Figures

List of Tables

List of Abbreviations

VC	Visual Cryptography
EVC	Extended Visual Cryptography
VCT	Visual Cryptography Technique
EVCT	Extended Visual Cryptography Technique
HVS	Human Visual System
R	Red
G	Green
B	Blue
C	Cyan
M	Magenta
Y	Yellow
RG	Red Green
GB	Green Blue
RB	Red Blue
RGB	Red Green Blue
CMY	Cyan Magenta Yellow
DWT	Discrete Wavelet Transform
LUB	Least Upper Bound
CTVCS	Color Transfer Visual Cryptography Scheme
DES	Data Encryption Standard
RSA	Rivest-Shamir-Adleman
CIT	Color Index Table
XOR	Exclusive OR
BW-VC	Black-and-White Visual Cryptography
CBW-VC	Color Black-and-White Visual Cryptography

Chapter 1

Introduction

This chapter discusses the importance and necessity of security and privacy of confidential data that we access on daily basis via Internet. This chapter also discusses the Visual Cryptography and Extended Visual Cryptography for black-and-white and colored images and their methodologies.

1.1 Importance of Data Security and Privacy in Digital World

Internet is the vast and major source of information through which multimedia data is exchanged to a large extent. This data can be the text, handwritten text, files, graphic objects, images, animation, audio, video and so on which may contain any secret or confidential information. Generally, data is exchanged through unsecured and untrusted communication medium, due to which chances of data breach increase. So, there is always a need to maintain the privacy and security of the data.

Online business, trading, marketing, shopping, education and e-commerce are increasing day by day at a very fast rate. These sectors include various online transactions which are made on daily basis through Internet. The transactions can be electronic funds transfer; making online payments through debit cards, credit cards and net banking; electronic documents transfer; exchanging sensitive information like bank account numbers, passwords and many more. This confidential and sensitive information are exchanged via untrusted medium with robust cryptographic algorithms. Maintaining the authorization and authentication of private data is a necessity. The medium or channel through which the data is exchanged can't be controlled, but robust and secure algorithms can be designed that would ensure complete

privacy and security of our data.

1.2 Cryptography and its Importance

All transactions include high level of privacy and security. The exchanged data may contain secret and confidential information which has to be transferred securely between intended parties. The communication medium through which data is exchanged is unsecure and untrusted, hence data can be attacked, breached or counterfeited during transfer. Therefore, Cryptography plays a very important role in exchanging the sensitive information.

Cryptography is an area in which the original data is transformed into another form which can't be perceived easily by anyone except the intended recipient. The original data is called *plain text* which is encrypted using a secret key to make the *cipher text*. The cipher text is encrypted and transformed form of plain text which can only be decrypted by the intended recipient using same or different key.

A key is used during encryption and decryption process. If the key is same for sender and recipient, it is called symmetric cryptography. If the key is different for sender and recipient, then it is called asymmetric cryptography. The key used in symmetric cryptography is secret or private key. While in asymmetric cryptography, two keys are used. One is secret or private key and other one is public key. Private key is kept secret to either sender or receiver and public key is publicly available.

The significance of VC is that no key is required in cryptographic procedure. The key used for encryption/decryption process is kept secret between the sender and receiver. Sometimes, it is registered to the trusted third party. The cipher text is exchanged through untrusted communication medium. The cipher text even if obtained by any non-trusted party can't be deciphered without key. The examples of various cryptographic algorithms are Data Encryption Standard, triple DES, Advanced Encryption Standard, Blowfish in which encryption and decryption are done by same key. RSA is the most popular algorithm for asymmetric cryptography in which encryption and decryption are done using different keys.

1.3 Visual Cryptography

Images are a vital form of multimedia content which is extensively exchanged over the Internet. So, there should be a secure and simple method to exchange images through

any unsecured medium. Hence, VC came into picture. VC is a vital field for sharing secret images conveniently without any use of key which is generally used by traditional cryptography techniques. It is an effective and simple way for sharing secret and confidential images. The VC initially proposed by Naor and Shamir (1995) is used to share secret images. In (k, n)-VCT, n shares (shadow images) of the secret image are generated during encryption and are sent through any untrusted medium. Out of n shares, any k shares are just stacked/ superimposed (using logical "OR" operation or "AND" operation depending upon which color is considered which bit) at the recipient's side to get the original secret image back. Any less than k shares would not regenerate the original secret image.

The basic technique is (k, n)-Visual Cryptography Technique which generates n shares corresponding to the original secret image. At least k-out-of-n shares are needed to reconstruct the secret image back. Any less than k shares would not be able to reconstruct the secret image even if any amount of computing power is available. The shares are random noise-like shares thereby revealing no information about the secret image except its size in some cases. The shares can be printed on transparencies and are distributed to n participants. Any k-out-of-n participants would agree to decrypt the secret image. The beauty of the technique is the decryption process, which can be done just by stacking/overlaying/ superimposing any k-out-of-n transparencies onto one another and observing the reconstructed image using Human Visual System (HVS), that is, human eye without any need of complex calculations and computations. The decryption process can be done by any person without having any knowledge of cryptography.

The decryption process is implemented by performing the logical "OR" or "AND" operation on the shares. The visual quality of the recovered image depends upon the technique used. Sometimes, contrast of the reconstructed image can be decreased up to 25% to 75% in case of black-and-white images.

1.4 Difference between VC, Steganography and Watermarking

1.4.1 Visual Cryptography

VC is an area particularly dedicated to the images in which the secret image content is stored in either meaningful or meaningless shares and can be decrypted easily with the HVS, that is, the human eye. No complex cryptographic calculations and computations are required to decrypt the image.

1.4.2 Steganography

Steganography, on the other hand, is an area in which any secret data is hidden as some other ordinary data. Secret data and ordinary data, both can be in the form of file, message, text, animation, audio, video, image, graphics object and so on. Moreover, the decryption process in Steganography is standard decryption process used in traditional cryptography techniques which is dissimilar to the one used in VC. Cryptography is the way of concealing the messages alone by converting them into another unintelligible form which can't be decrypted easily. Steganography takes advantage of cryptography by concealing the secret message into another ordinary message thereby giving more security. Steganography has important application in transmission of computer files which make the transmission of files more secure as compared to normal Cryptography.

1.4.3 Watermarking

Watermarking is the method for embedding the data into some protected data especially to show the ownership of the protected data. Data can be any multimedia data. The size of the embedded data is generally small. Watermarking is extensively used in copyright protection. When data is copied in any form, watermaking can be used to recognize the right owner of the data.

Stegnaography and Watermarking are technically similar but Steganography more focuses on imperceptibility while watermarking more focuses on robustness. Imperceptibility is the property in which it becomes very difficult for HVS to distinguish between the original image and the embedded one. Robustness is the property in which the watermark can be extracted from the protected image, even after it has suffered various attacks during transmission.

The difference between VC, Steganography and Watermarking is given Table 1.1 on the basis of following parameters:

i Area/Field description (purpose)

ii Encryption procedure

iii Decryption procedure

iv Whether the key is required in cryptographic procedure or not

v type of data shared in every field

vi application area

Table 1.1: Difference between VC, Steganography and Watermarking

Field	VC	Steganography	Watermarking
Purpose	sharing secret and confidential images by making shares (shadow images)	sharing private data by hiding it into some other ordinary data	hiding ownership information into some data to identify right owner of the data
Encryption procedure	generating the shares of the image which is to be shared	embedding secret data into ordinary data	Embedding a watermark into owner's data
Decryption procedure	stacking significant number of shares to get the original image	extracting the hidden private data from ordinary data	extracting the watermark to identify the owner
Key Required	no	yes	yes
Type of data	any pictorial, handwritten or textual images	text, message, images, audio, video, animation, graphic objects and so on	text, message, images, audio, video, animation, graphic objects and so on
Application area	where a lot of work is done with images like medical sciences, geographical sciences, aeronautical sciences and so on	In any field where security and privacy are major factors	especially to identify the owner of the work like copyright protection

1.5 Extended Visual Cryptography

The generated shares in VCT are random noise-like shares with no individual meaning while in EVCT, the shares are meaningful, that is, the shares would be seen as some meaningful images. Each share actually contains some partial information of the original secret image embedded with a cover image. The cover images give meaning to the shares that improves the security and reduces the chances of attacks on shares. Hence, it is concluded that EVC is more secure than VC.

The shares can be distributed to n recipients through any unsafe communication medium. If any intruder gets any k - 1 or less than k - 1 shares would not be able to perceive the information within the shares except size of the image in some cases.

There is another way of performing VCT in which participation of one or more shares can be fixed for decrypting the original image. Any subset of shares that is generating the original secret image is regarded as *qualified subset*. The subset which is not able to generate

the original secret image is regarded as *forbidden subset*. The set of qualified subsets is known as *qualified access structure* and set of forbidden subsets is known as *forbidden access structure.*

1.6 Main Aspects in VCTs and EVCTs

I **Contrast:** Contrast of the recovered image should be good enough so that the data in the recovered image would be easily perceived by the recipient. Directly overlaying of shares reduces the contrast of the recovered image. In (k, n)-VCT of black-and-white images proposed by Naor and Shamir (1995), the contrast is reduced by half as compared to the original secret image. The contrast of the regenerated image depends on the type of technique applied on different kinds of images.

II **Security:** In (k, n)-VCT, any fewer than k shares would not reveal any information about the original secret image even if any amount of computing power is available. The shares are sent through the unsecure communication channel after encryption. There are always the chances that intruder would try to breach the information hidden in the shares. The shares should be as secure as possible, so that even if the intruder obtains the shares, he will not be able to unhide and access the information from the shares. EVCT increases the security of the shares by making them meaningful by embedding cover images into them. These embedded shares are called *camouflage images*.

III **Pixel Expansion Ratio:** Each pixel from the original secret image is expanded to m number of sub-pixels depends upon the requirements and the technique used. Sometimes pixel expansion is not performed at all to keep the size of shares small but it affects the resolution. Also, larger values of m increase the size of the shares which requires more space to store the shares and more time to transmit them. So, m should be as small as possible. On the other hand, if someone needs more resolution or contrast of the recovered image, more pixel information has to be stored in the shares and larger values of m are needed. Hence, a trade-off is required between the contrast of the recovered image and size of the shares.

IV **Storage Space and Transmission Time:** More the size of the shares, more storage space would be required to store the shares. In VCT or EVCT, shares are communicated via transmission medium instead of the actual image itself. The space to store the shares might not be available easily. So, the size of the shares should be as small as

possible. The size depends upon the pixel expansion ratio. Less the pixel expansion ratio, less will be the size of the shares. Also, the time to transmit the shares decreases if the size is small.

V **Nature of Shares:** The shares can be seen as either random noisy images or some meaningful images. Making the meaningful shares increases the security and reduces the suspicion that something is hidden in the images. VC generates noisy shares and EVCT generates meaningful shares. To make shares meaningful, other non secret or non confidential images are required, which are called cover images. The secret content hidden with cover images are known as camouflage images.

VI **Decryption:** The beauty of VC is its decryption process which is performed just by stacking the significant number of shares by using logical "OR"/"AND" operations unless in traditional cryptography which needs a key to decrypt the data. The shares can be laid down on transparencies and those transparencies can be correctly superimposed and aligned to decrypt the original image. The drawback of this process is that, it gives reduced contrast of the recovered image. Sometimes, additional computer support can be required to enhance the visual quality and contrast of the recovered image. "XOR" operation can be used to improve the contrast.

VII **Number of Secret Images Shared At A Time:** Mostly, all the techniques share a single black-and-white, gray-scale or true colored image at a time. To share more number of images at a time, more information is required to store in the shares, more complex the cryptographic procedure would be, more computer support would be required during the decryption process.

VIII **Generality:** Generally, VCT or EVCT is (k, n)-secret sharing techniques but they can't be generalized to higher values of k and n. As the value of k or n increases, more shares would be generated, more the number of participants would be, more complex would be the decryption procedure.

1.7 Methodology for VCT and EVCT

1.7.1 Step by step Methodology of VCT

i Select the secret image which is to be shared.

ii Select the values of n and k.

iii Generate n shares by optionally using pixel expansion. If pixel expansion is done, then the shares would be having size larger than the secret image size. Hence, the share would be having total of m pixels.

iv Distribute the shares to n recipients.

v Recipients would lay down the shares on transparencies.

vi Select qualified subset k out of n shares (transparencies) to regenerate the original image back.

vii Those k participants would stack/superimpose their transparencies to reconstruct the original image.

1.7.2 Step by step Methodology of EVCT

i Select the secret image which is to be shared.

ii Select the values of n and k.

iii Select a different cover image for every share.

iv Generate n shares using pixel expansion by embedding cover images in them. As pixel expansion is done, the shares would be having size larger than the secret image size. Hence, the share would be having total of m pixels.

v Distribute the shares to n recipients.

vi Recipients would lay down the shares on transparencies.

vii Select qualified subset k out of n shares (transparencies) to regenerate the original image back.

viii Those k participants would stack/superimpose their transparencies to reconstruct the secret image and the effect of cover images would be nullified into the resultant original image.

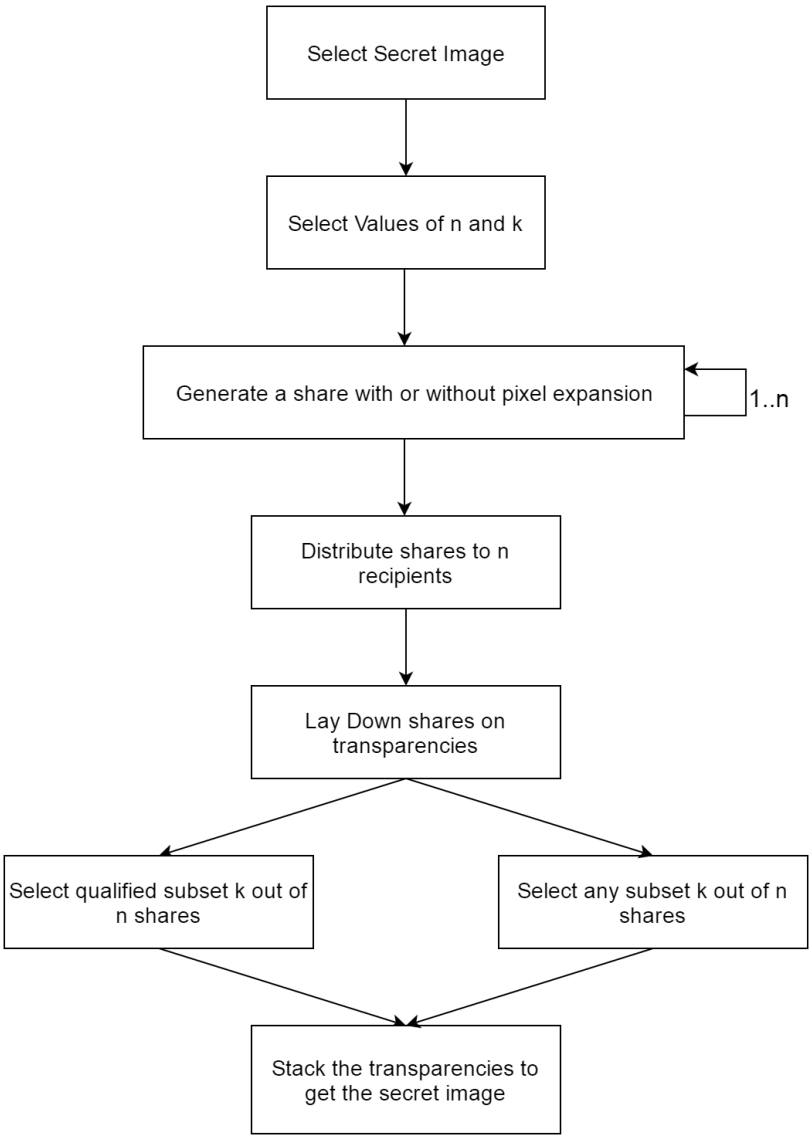


Figure 1.1: Methodology of VCT

1.8 VCT for Binary Images

(k, n)-VCT secret sharing technique can be implemented as (2, 2)-VCT secret sharing technique in which 2-out of-2 shares would be needed to generate the original secret image. The original secret image consists of black-and-white pixels, in which each pixel is handled separately. The secret image can be reconstructed by superimposing the shares. The pixel expansion in shares is optional, that is, it depends upon the requirement and the technique used. Pixel expansion increases the size of the shares and increases storage space and time to transmit the shares.

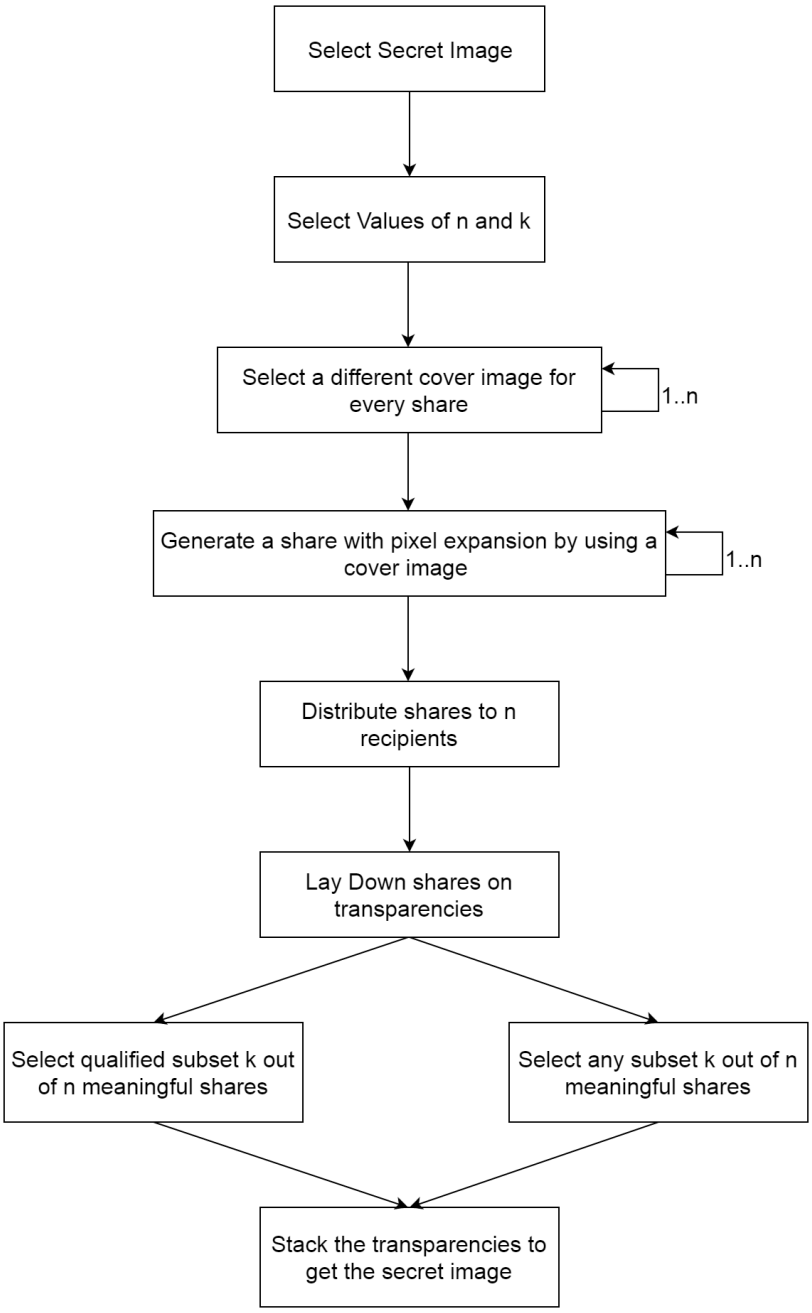


Figure 1.2: Methodology of EVCT

Each pixel in original image can be expanded to any number of sub-pixels. After expansion, each share is having total of m sub-pixels. The original image can be reconstructed by overlaying/superimposing shares on one another either by performing logical "OR" operation or "AND" operation, depending upon which color is considered as which bit. "OR" operation is performed when 0 is taken as white colored sub-pixel and 1 is taken as black colored sub-pixel. "AND" operation is performed when 0 is taken as black colored

sub-pixel and 1 is taken as white colored sub-pixel. The overlaid/stacked image can have a reduced contrast. If a particular number of sub-pixels in the stacked image are greater than a predefined threshold, then the whole pixel would be considered as black otherwise the pixel would be considered as white. For example, say a pixel is divided into 9 sub-pixels. The value of m is 9. The threshold value defines the minimum number of black sub-pixels. The threshold value is set to 5. Now, if a pixel in the resultant stacked image contains less than 5 black sub-pixels, the pixel would be considered as white. If a pixel contains greater than or equal to 5 black sub-pixels, the pixel would be considered as black.

The contrast of the reconstructed image depends upon the total number of black and white pixels in resultant stacked image corresponding to the original image.

1.9 EVCT for Binary Images

(k, n)-EVCT secret sharing technique can be implemented as (2, 2)-EVCT secret sharing scheme in which 2-out-of-2 shares would be required to generate the original secret image. As the shares in EVCT are meaningful, there is a need for cover images which are to be embedded into the shares during encryption to make them meaningful. The original secret image, cover images and shares are all black-and-white images.

During decryption, the shares are stacked to get the original secret image and the visual effect of cover images is nullified in the resultant stacked image. There would be a contrast reduction in shares as well as in the stacked image.

1.10 VCT for Colored Images

The original secret image consists of colored pixels in which each pixel is handled separately. Each pixel can be of any number of bits depending on the number of colors in the image. More the number of colors/pixels, more would be the number of colors in the image. For example, there would be 8 bits/pixel in 256 color image and there would be 24 bits/pixel in an RGB image. Pixel expansion has to be done in this technique. The shares can be generated by expanding every 8-bit pixel to 3×3 sub-pixels block and every 24-bit pixel to 5×5 sub-pixels block. All these 8 bits can be stored in a 3×3 block. First 8 blocks are used to store pixel information and last 9th block can store the additional information like palette data. The case for 24-bit pixel would be similar with the technique described for 256 gray-scale images .

The secret image can be reconstructed by superimposing significant number of the shares. The recipients may need to perform some additional work besides overlaying the shares. For example, there may be the case that the recipients get a random noise like stacked image and with the help of colormap sent by the sender, the recipients obtain the original image. The colormap is used for mapping the stacked image to the original secret image.

1.11 EVCT for Colored Images

EVCT for colored images can be performed by first making the random noise-like shares by using VCT and then embedding cover images into them to make them meaningful. The original image and cover images would be the colored images. The generated shares can be black-and-white or colored. The reconstructed image from the shares would be the colored one.

During decryption, the meaningful shares are stacked to get the original secret image and the visual effect of cover images is nullified in the resultant stacked image. There may be additional work done at the receiver side. For example, a colormap can be used for mapping along with the stacked image to get the original image.

1.12 Dissertation Organisation

Chapter 2: This chapter discusses the work done by various researchers in the field of VC and EVC. The chapter also describes the evolution of techniques from black-and-white to colored images.

Chapter 3: This chapter describes the problem statement based on various cryptographic aspects, motivation and contribution of the proposed work.

Chapter 4: This chapter presents the two proposed EVCTs with algorithmic details, their implementation and experimental results.

Chapter 5: This chapter concludes the work done in this dissertation and proposed further improvements which can be done in existing proposed techniques.

Chapter 2

Literature Survey

This chapter discusses the work done on VCTs and EVCTs by various researchers. The evolution of VCTs and EVCTs from binary to colored images is also discussed in this chapter.

2.1 Introduction

The contrast, resolution and visual quality of the reconstructed image after decryption process should be as much as possible, because only then the user would be able to retrieve the required information from the image. Decryption in VC for black-and-white images is the easiest process which is done merely by stacking/overlaying the appropriate number of shares to get the original secret image back. But, there is a drawback of the technique that it produces the reconstructed image with contrast reduction thereby reduces the visual quality of the image. Researchers proposed various techniques to enhance the visual quality and resolution of the reconstructed image.

The security is improved by making shares meaningful which reduces the suspicion that something is concealed in the share images. Various EVCTs for black-and-white and colored images are proposed by researchers, to not only enhance the visual quality of the recovered image but the shares also. The drawback of making shares meaningful is that we need additional images to be embedded into the shares called cover images. More memory is required to store the cover images. Also, to make good quality shares and get the high resolution of the recovered image, more pixel information of the original secret image has to be stored in the shares which again requires more memory. The drawback of increasing the memory space is that it would require more time to transmit the shares from one side to the other, which becomes less efficient for real time systems. So, the researchers proposed

different techniques to shares images focusing on every possible aspect of the VC.

2.2 Related work in the area of VCTs

VC was initially proposed by Naor and Shamir (1995) as (k, n)-secret sharing technique for black-and-white (binary) images. The technique is also referred to as k-out-of-n-VCT. The proposed technique is secure and easy to implement. Any k-out-of-n shares can regenerate the original secret image but with 50% reduction in contrast. Any fewer than k shares would not generate the original secret image. The shares of the original secret image are generated and sent through any unsecure communication medium. The secret image can be reconstructed just by stacking/overlaying (using logical "OR" operation) the shares without performing any complex cryptographic calculations. The original image can be analyzed just by the HVS that is, the human eye. The beauty of the scheme is its decryption process. No cryptographic knowledge is needed to decrypt the image.

Initially, the technique is implemented as (2, 2)-VCT in which 2-out-of-2 shares are needed to recover the original secret image. The generated shares are random-noise like shares. Single share can't reveal any information about the original secret image. Each pixel in the original secret image can be expanded to any number of sub-pixels. After expansion, each pixel would be having total number of m sub-pixels. Secret image consists of only black-and-white pixels. Each pixel is handled independently in the original image. Out of two shares which are generated, one can be regarded as *cipher image* and other one can be *key share*. By stacking/superimposing the shares (transparencies) onto one another, one can easily reconstruct the original secret image back.

The model (2012) can be described as an $n \times m$ boolean matrix 'S' which is shown in equation 2.1. The structure of S can be described as:

$$\mathbf{S} = (\mathbf{s}_{ij})_{n \times m} \tag{2.1}$$

as described in (2012), Where $s_{ij} = 1$ or 0 iff. the jth sub-pixel of the ith share is black or white respectively.

The Hamming weight H(V) represents the total number of black sub-pixels in the recovered image and is given by "OR"ed m-vector V which is interpreted by the visual system as follows:

A black pixel is interpreted if H(V) $\leq d$ and white if H(V) $< d$ - αm for some fixed threshold $1 \leq d \leq m$ and a relative difference $\alpha > 0$.

Where, d is predefined threshold, α is contrast of the recovered secret image, m is number of sub-pixels/pixel, n is total number of shares generated.

The construction of the shares is illustrated using the above model by a 2-out-of-2 VCT ((2, 2)-VCT). The collections of 2×2 matrices are:

$C_0 = \{$all the matrices obtained by permuting the columns of $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\}$

$C_1 = \{$all the matrices obtained by permuting the columns of $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\}$

Where, $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ is base matrix M_0 and $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is base matrix M_1.

The shares are generated by taking any matrix from C_0 and C_1 corresponding to white and black pixel from the original secret image. When both shares are overlaid and correctly aligned onto one another, the original secret image will be revealed.

Figure 2.1 (2015) shows the pixel expansion, that is, total number of sub-pixels per pixel in the shares. From the original secret image, every pixel is converted into two sub-pixels in the shares. Out of 2 sub-pixels, one is having black color and the other one is having white color. The stacked image can be reconstructed either by “OR” operation or by “AND” operation depending upon which color is considered as which bit. “OR” operation is performed when 0 is taken as white colored sub-pixel and 1 is taken as black colored sub-pixel. “AND” operation is performed when 0 is taken as black colored sub-pixel and 1 is taken as white colored sub-pixel.

VCT for black-and-white images produces the resultant secret image with 50% reduction in contrast due to “OR” or “AND” operation. For getting the resultant image same as the original image without reduction in contrast, “XOR” operation is used in place of “OR” and “XNOR” operation is used in place of “AND”. Each pixel of the original black-&-white image is converted to 1-black-1-white sub-pixel in the share image and hence the resultant images are having size greater than the original image. Figure 2.2 (2015) shows the single pixel of secret image and pixel expansion with 2 sub-pixels. Finally, Figure 2.2 shows the

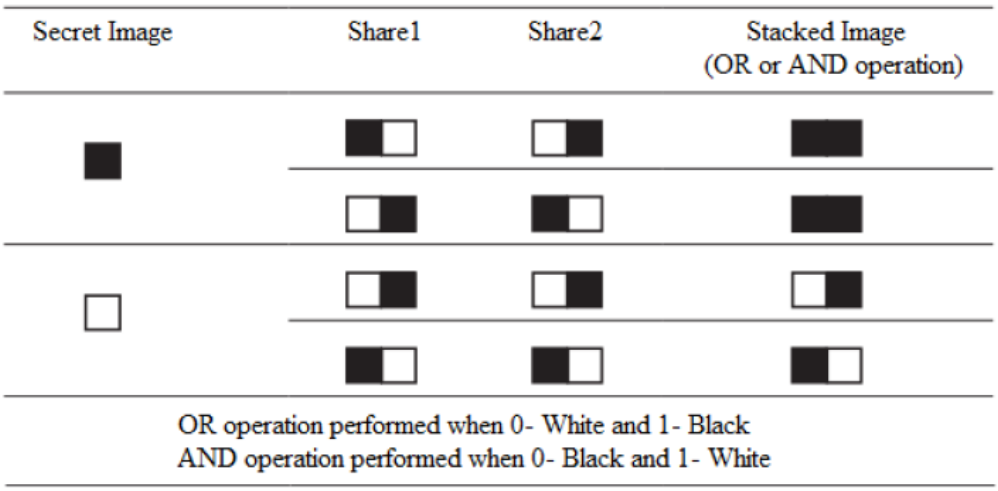


Figure 2.1: VCT for single black/white pixel with pixel expansion by 2 pixels by using "OR"/"AND" operation.

resultant pixel color using "XOR"/"XNOR" operation. Figure 2.3 shows the implementation of the technique on black-and-white image. Figure 2.3a shows the black-and-white original image, 2.3b and 2.3c shows binary share1 and share2 respectively, 2.3d describes the stacked image using "OR"/"AND" and 2.3e presents the stacked image using "XOR"/"XNOR" operation.

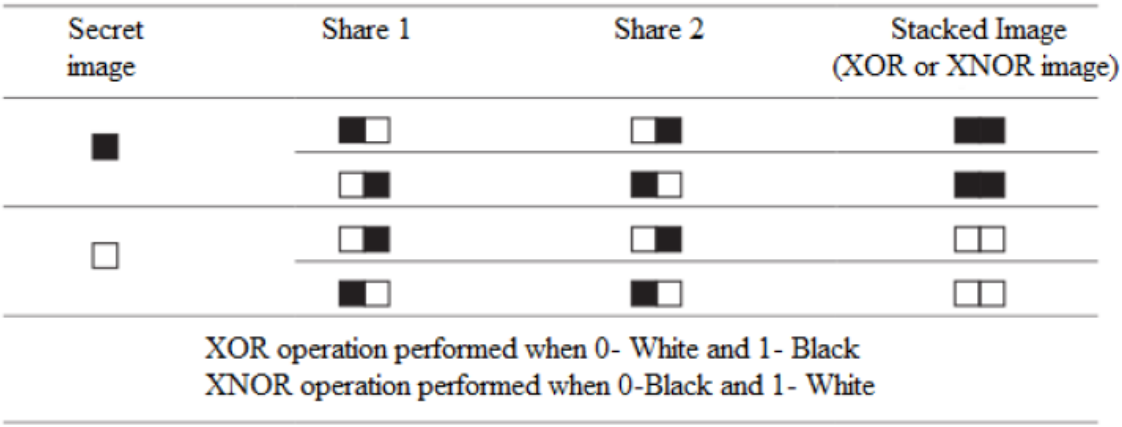


Figure 2.2: VCT for single black/white pixel with pixel expansion by 2 pixels by using "XOR"/"XNOR"

A Circular Colored VCT is proposed by Verheul and Tilborg (1997) which is a k-out-of-n technique in which c-color secret image can be shared. Each pixel in the secret image is expanded to b sub-pixels. Further each sub-pixel is divided into c colored regions and each

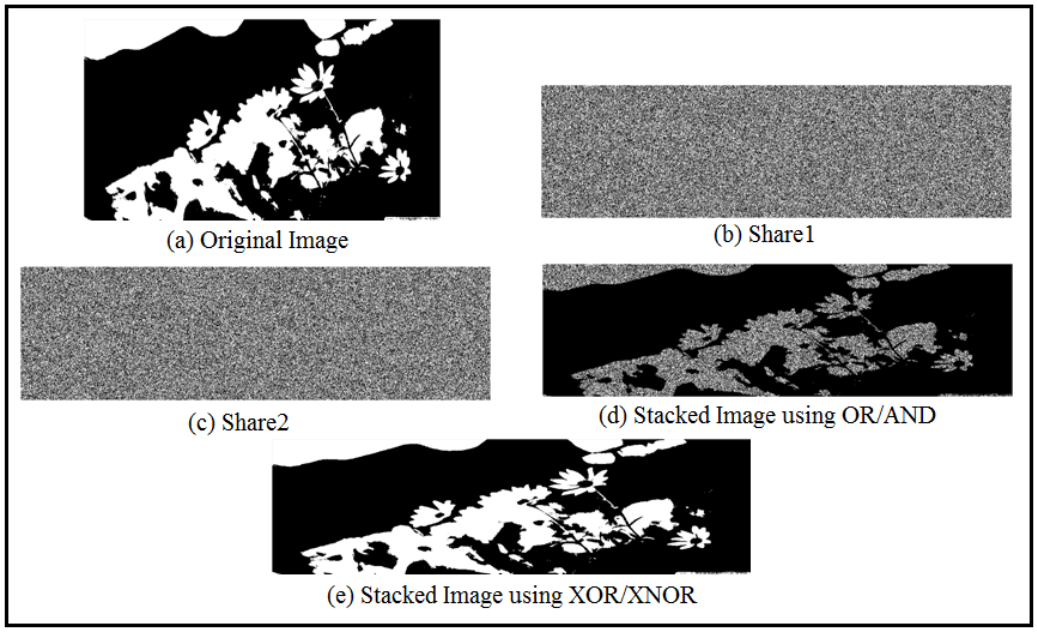


Figure 2.3: VCT for black-&-white image

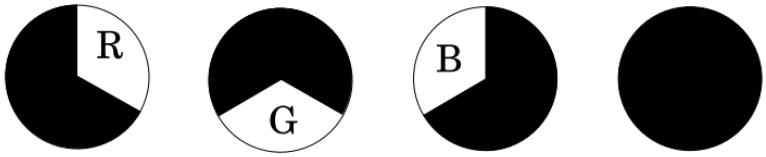


Figure 2.4: Representation of three colors

colored region is a sector of a circle with angle $2\pi/c$. The sub-pixel is said to be of color i when ith sector of the sub-pixel is having the color i and the remaining portion is black. Each pixel of the secret image would be present in each share in the form of b sub-pixels. The color of the pixel obtained from stacking the shares would depend on the "OR" operation of the corresponding sub-pixels. The color i of a sub-pixel would be obtained after stacking any k-out-of-n shares, if and only if all the k shares are having color i sub-pixels, otherwise, it would be seen as black. The drawback of the scheme is that, increase in number of colors would result in decrease in resolution, due to color density in the pixel in the shares. Three colors (R, G and B) are represented in the Figure 2.4 (1997).

Koga and Yamamotq (1998) proposed the (k, n)-VCT for gray-scale and colored images by using lattice based concept. Any colored image with J distinct colors can be shared using given technique. Each pixel is converted into horizontal block of m number of sub-pixels. The color of the block with m sub-pixels is assigned at a certain position. The color of the

stacked image would be recognized by only one sub-pixel while all other sub-pixels would give either white or black color. The predefined lattice is used to perform the stacking of the shares. The lattice would change according to the number of colors used in the technique. When shares are overlaid, LUB of the values of sub-pixels from the lattice is carried out. As the colors in the original image increases, the resolution of the recovered image decreases.

On increasing the number of colors, the contrast of the recovered image decreases rapidly and the techniques cannot be extended to the EVCTs. This is the major drawback of the above scheme.

Chang *et al.* (1999) proposed a VCT for sharing a secret image with very less number of colors. The technique uses 3×3 pixel expansion ratio to share a secret image having 5 colors only. The technique uses logical "AND" operation for decryption. Now-a-days colored images are more in use than the images with fewer colors.

The contrast devised by Naor and Shamir in (1995) is given by equation 2.2 which is exponential.

$$(2e)^{-k}/\sqrt{2\pi k} \tag{2.2}$$

As the value of k increases, the contrast of the stacked image decreases exponentially which is the drawback of the proposed technique. To optimize the contrast, Hofmeister *et al.* (2000) proposed the technique using linear programming showing the linear relation between the minimum number of shares required to get the secret image back that is, k and contrast of the stacked image. As the value of k increases, the contrast would decrease linearly which is much less than the one proposed in above scheme.

Lin (2000) proposed a technique for sharing a secret image with 256 colors using logical "AND"/"OR" operations. The drawback of the technique is that, a mask share is needed to decrypt the image, although it is used to enhance the security of the overall technique.

Hou (2003) proposed three different (k, n)-VCTs for gray-scale and colored images using halftoning technique and CMY color decomposition method. In first method, C, M and Y components of the image are extracted and are converted into the halftone images. The haftoned images are the shares with 2×2 block pixel expansion. The images (shares) are combined to form the composed image. Then each pixel from the composed image is encrypted using the proposed table. Decryption can be done using stacking of three shares and an additional mask share which is drawback of the method. The stacked result of

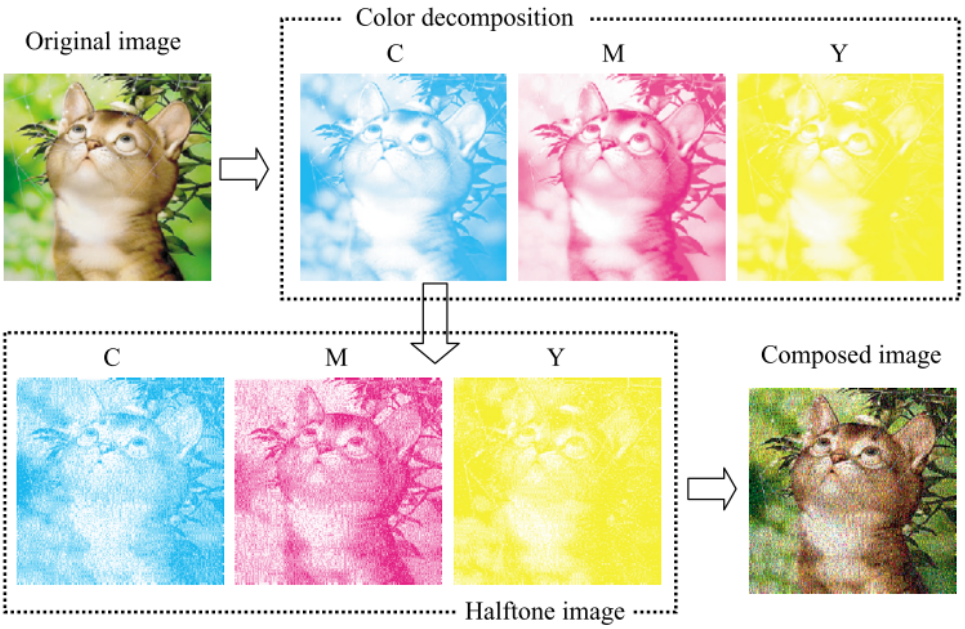


Figure 2.5: Generation of composed image

the first method is a non-continuous halftoned image. The method is shown in Figure 2.5 (2003) and 2.6 (2003). Figure 2.5 shows the construction of composed image. Figure 2.6 shows the C share, M share, Y share, mask share and stacked result is the Lina image. Also, the image uses 8 different colors. The technique is also applicable to the binary images.

In second method as shown in Figure 2.7 (2003), the technique is similar to the first but the proposed table is changed to decrease the number of shares used in decryption in first method. This reduces the contrast of the stacked image. Figure 2.7 shows share1, share2 and the resultant stacked result. The third method as shown in Figure 2.8 (2003), removes the drawbacks of the above two methods. Neither all four shares are required to get the result nor contrast much compromised.

Jin *et al.* (2005) proposed (2, 2)-Progressive VCT for color images as shown in Figure 2.9 (2005). They described a single encryption process of a secret image using Halftoning and a novel Microblock Encoding Scheme as shown in Figure 2.9c and 2.9d. The decryption process is carried out in three separate ways resulting in the difference in visual quality of the recovered images. Recovered image resolution and contrast would vary in three different decryption ways. First decryption process, as shown in Figure 2.9e and 2.9f, is the traditional stacking of (two) shares using both “OR” and “XOR” operation. Second process, as shown in Figure 2.9g, would give halftoned quality image. Last process, as shown in

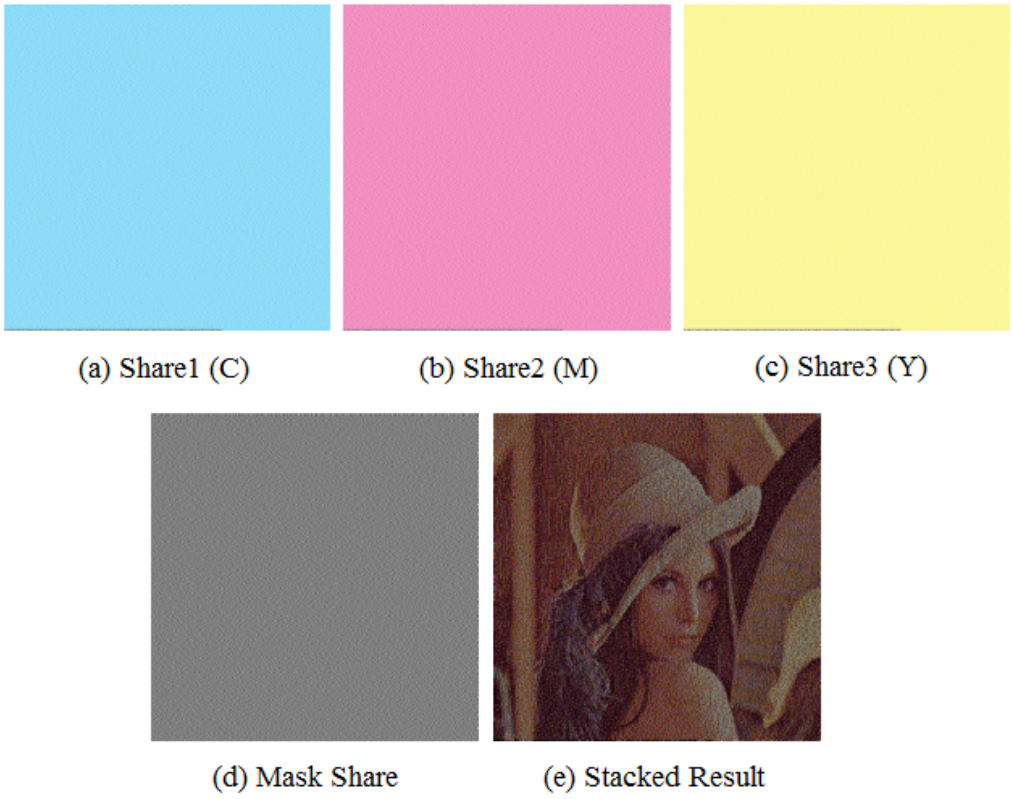


Figure 2.6: Decryption Method 1

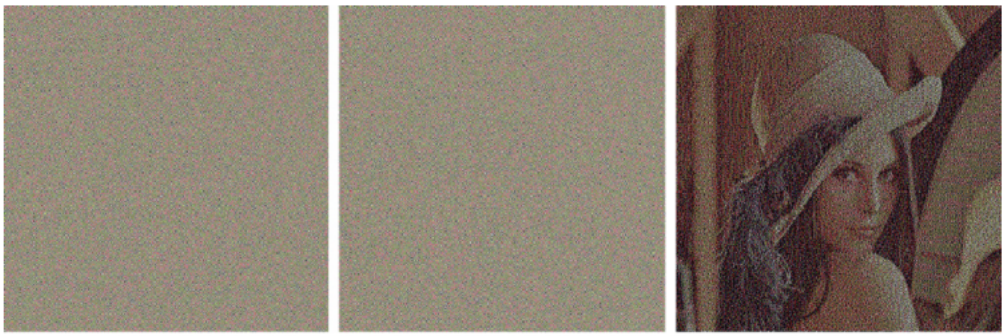
Figure 2.9h, would include some decryption computations giving the best possible quality image. “XOR” is used to enhance the quality.

Chao and Lin (2006) proposed a (2, 3)-threshold VCT using CMY color decomposition method and error injection. The true color 24-bit original secret image is converted into three 1-bit halftone images C, M and Y or a single 3-bit C-M-Y halftone image. The concept of three vectors {{C, M, 0}, {C, 0, Y}, {0, M, Y}} is used to generate the shares. Each pixel P_{ij} (containing C_{ij} , M_{ij} , Y_{ij} component) in 3-bit halftone image is expanded to nine 2×2 blocks ($C1_{ij}$, $C2_{ij}$, $C3_{ij}$, $M1_{ij}$, $M2_{ij}$, $M3_{ij}$, $Y1_{ij}$, $Y2_{ij}$, $Y3_{ij}$). Any 2-out-of-3 shares can generate the original secret image. The drawbacks of the technique are that the recovered original secret image is noisy and the technique is not lossless.

In (2007), Klein and Wessler proposed a technique in which any subset of P (group P of n recipients) shares a particular secret. It can be said that every subset of shares is *qualified subset* in anyway. No subset of shares is *forbidden subset*. The generated subsets would be less than 2^n-1 with minimal pixel expansion ratio and a good contrast.

(a) Share1 (b) Share2 (c) Stacked Result

Figure 2.7: Decryption Method 2



(a) Share1 (b) Share2 (c) Stacked Result

Figure 2.8: Decryption Method 3

Lou *et al.* (2007) proposed a technique in which VC is used in copyright protection using watermarking. They proposed a method in which watermark need not be embedded in any image but it is used to generate a secret image and a public image. The scheme is divided into two steps. First step is generating the secret image and second is watermark extraction. The secret image is generated using a protected image, original watermark, a secret key and a predefined codebook. The technique uses DWT to extract the feature value which is further used in secret image generation. Then secret image is registered to the certified authority. In second step, the public image is generated using suspected image, secret image, a secret key and a predefined codebook. The public image is available publicly. Finally, the watermark can be extracted by performing logical "XOR" operation of secret and public image.

In (2009), researchers proposed a technique in which a secret image is first encrypted using a symmetric key and then its shares are generated. The decryption can't be carried out only by stacking the shares, the key is needed to reveal the secret image. The key is used to

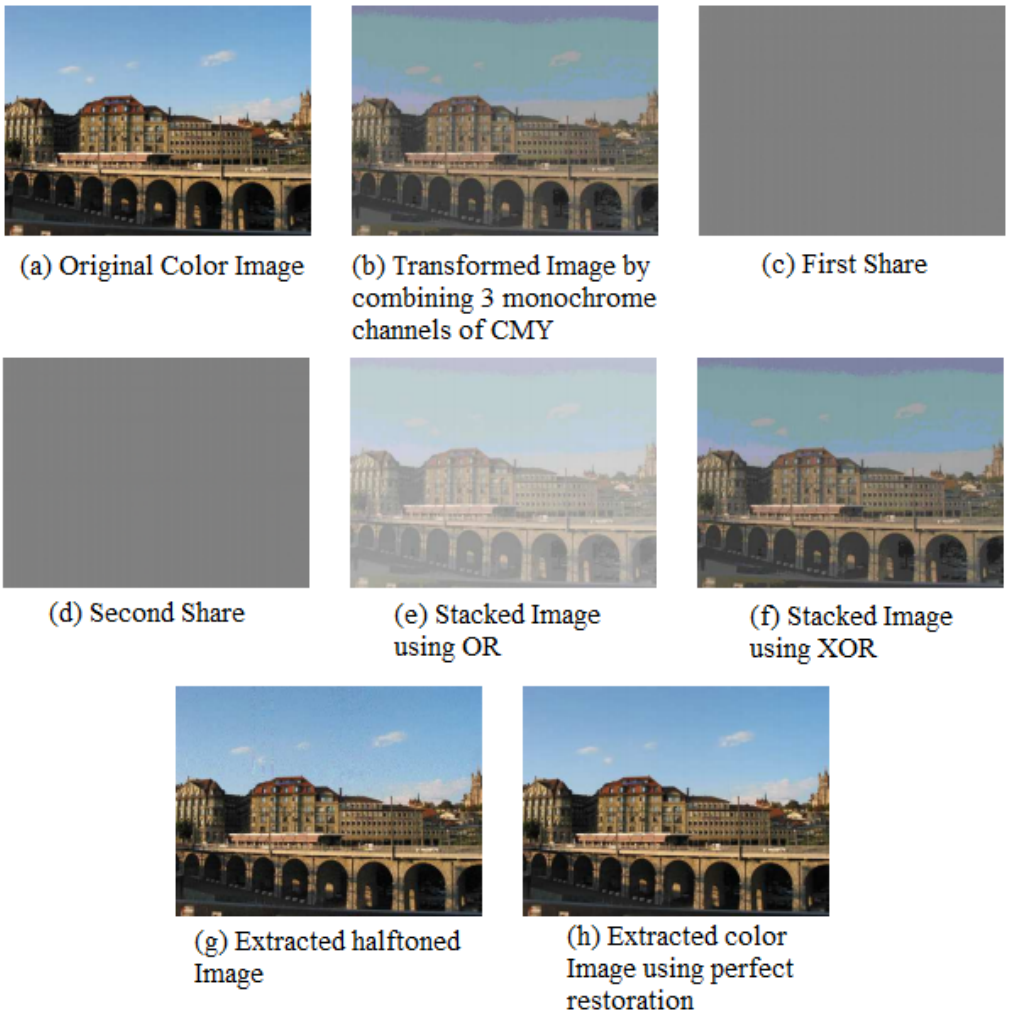


Figure 2.9: Image restoration by three decryption methods

increase the security of the sharing technique. The drawback of the technique is that it does not perform the decryption according to the conventional Visual Cryptography decryption procedure.

Kandar and Dhara (2011) proposed a (k, n)-VCT using random sequence generation for colored images. Each pixel of the original secret image consists of 32 bits because each pixel is having four components alpha, red, green and blue. In encryption process, if the original image is having 1 at a particular bit position in the pixel, then n - k + 1 shares would be having 1 at the corresponding bit position in the pixel and remaining k - 1 shares would be having 0 at that position. Hence, if original image is having 1 at a particular bit position then there are ${}^{n}C_{k-1}$ different sequences that can be generated for all the shares. All n shares are generated in this way. For decryption process, any k-out-of-n shares are stacked

Secret Image	Image Dimensions
	Secret Image 1 : 'SMIT' Dimension: 6 × 36 pixels
	Secret Image 2 : 'AND' Dimension: 12 × 36 pixels
	Secret Image 3 : 'SMIMS' Dimension: 24 × 36 pixels

Figure 2.10: Secret images and their dimensions

using logical "OR" operation to get the original secret image which can be analyzed by HVS.

Prisco and Santis (2013) proposed a (2, n)-CBW-VC secret images which is an improvement over normal BW-VC. The CBW-VC scheme used $\lceil log_3 n \rceil$ pixel expansion which is 1/3rd as compared to the pixel expansion in BW-VC. Also, it is not possible to construct (2, n)-CBW-VC for $n > 4$ and (k, n)-CBW-VC for $k > 3$. The generated shares in the technique are colorful random noise-like shares. The stacked image gives black color, as it is corresponding to the black color in original secret image. But, white color would be random noise like combination of colors in shares. Hence, the contrast is decreased in the stacked image. The researchers also described the improvement in the contrast with the use of full intensity colors.

The technique proposed by Lee *et al.* in (2014) is Visual Secret Sharing scheme without changing any size of the images in between the encoding/decoding procedure. The scheme regenerates the brighter, darker secret images with higher contrast.

The technique proposed by Lou *et al.* (2014) is (k, n)-VCT in which n binary noise-like shares are generated as shown in Figure 2.12 (2014). Figure 2.12a, 2.12b and 2.12c shows the three generated shares. Any qualified set of k binary shares can generate a high quality colorful version of the original image. Stacking result of share1 and share2 is shown in

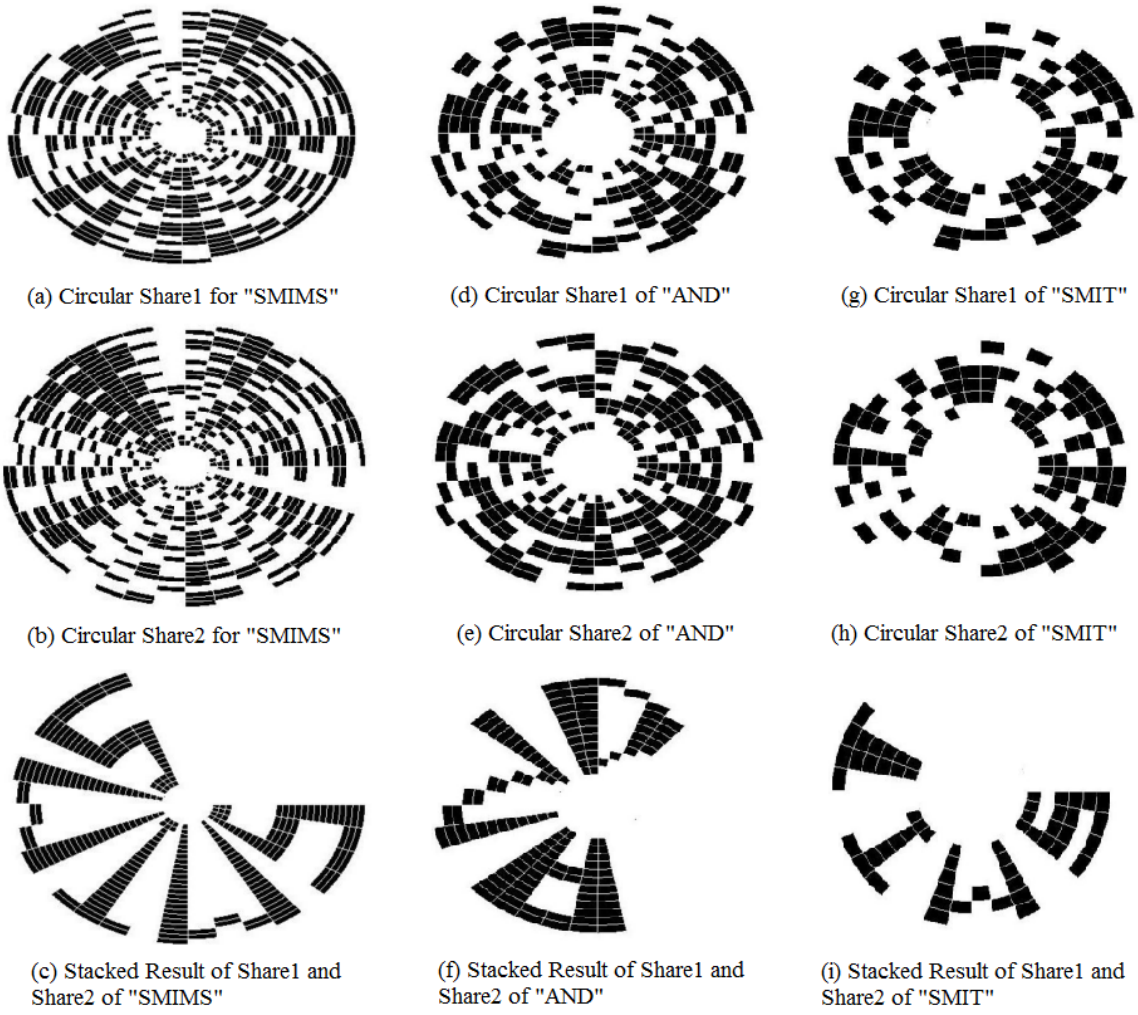


Figure 2.11: Circular Visual Cryptography

Figure 2.12d, of share1 and share3 is described in Figure 2.12e and of share2 and share3 is described in Figure 2.12f. The shares are first stacked to get the gray-scale halftoned version of the original image as presented in Figure 2.12g using HVS and then gray-scale version is converted into the colorful halftoned version, which is shown in Figure 2.12h, using less computation complexity. Further to improve the visualization, the colorful halftoned version of the original image is converted into the continuous tone version, as shown in Figure 2.12i, as the final output. The drawback of the technique is that it, generates the noise-like shares instead of meaningful images. The nature of recovered image is lossy. It also uses a key during encryption and decryption phases which is actually not a threshold technique with perfect security. So Yang *et al.* (2017) proposed the (k, n)-CTVCT. The technique achieves all results of (2014) without using a key. This technique produces binary shares same as in (2014).

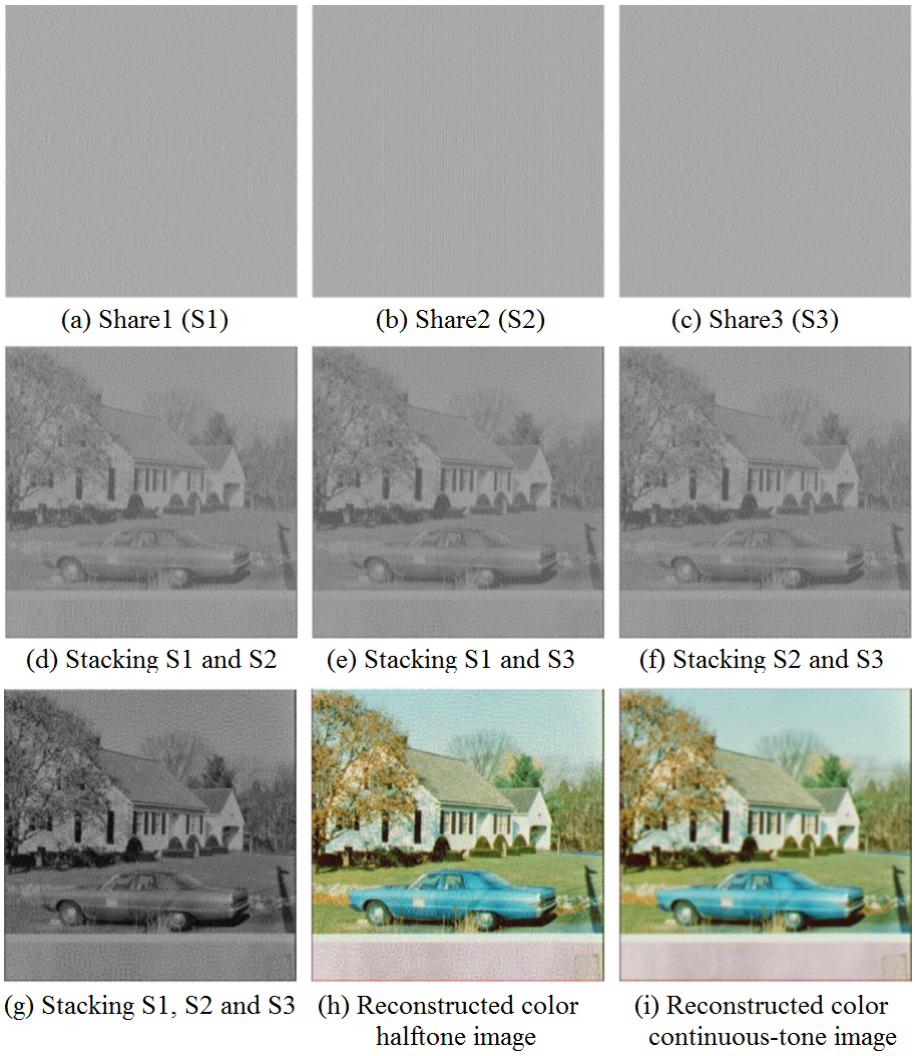


Figure 2.12: CTVCT

Gurung *et al.* (2014) proposed a (2, 2)-circular VC for binary images which is shown in Figure 2.10 (2014) and 2.11 (2014). The benefit of the technique is that n binary secret images can be shared at a time. The secret images can be stored in a single concentric circular plate. The images are stored in the increasing order of dimensions as shown in Figure 2.10. Every image would be having the dimensions double than the previous image stored. Firstly, an image with lowest dimensions is stored, then image having dimensions double than the previous image is stored and so on. Share1 is generated randomly while share2 is generated using a proposed algorithm. In the encryption process, initially share1, as shown in Figure 2.11g, and share2, as shown in Figure 2.11h, of first image is created, then share1 is concatenated (horizontally or vertically) with share2 to make the share1, as shown in Figure 2.11d, of second image. Now, share2 of second image, as shown in

Figure 2.11e, is generated using algorithm. The procedure continues until all the images are stored in the grid. The gird is converted to the concentric circular plate and two final circular shares are generated. Decryption is the reverse procedure of encryption. The secret image with the largest dimensions is extracted first, as shown in Figure 2.11c, then image having dimensions half than previous image is extracted, as shown in Figure 2.11f, and the procedure continues until all the secret images are extracted. The decryption is done by stacking the shares with correct alignment without any cryptographic calculations.

Pooja and Lalitha (2014) proposed a (2, 2)-VCT for halftone images. The technique requires computer support for decryption. The decryption is also performed by stacking the shares. The technique is proposed for gray-scale images and colored images using pseudo randomization and pixel reversal approach. Also, the dimensions of the original secret image and the regenerated image would be the same. Karolin and Meyyapan (2015) proposed a Color VC using RGB based secret sharing technique which is (2, 2)-"XOR" based VC.

Wei *et al.* (2015) proposed (2, 2)-VCT and (2, 2)-EVCT for gray-scale and colored images. The decryption process uses logical "XOR" operation instead of "OR" operation which gives the regenerated image without any loss in contrast. The white pixel appears complete white and black pixel appears complete black in the recovered image. However, the pixel expansion is there in the technique.

Figure 2.13: VCT for 256-color secret image

The VCT for 256-color secret image is discussed here. For showing 256 colors, there is a need for 8 bits to store the index of the color. So, each pixel of secret image is converted to 3×3 sub-pixel block in the shares where first 8 bits of the block makes the index of the color and last 9th bit shows the palette bit in share1 and used to adjust the number of black

colored pixels in share2 during encryption. Each share is having 4 white colored and 5 black colored pixels. The color along with the index number is stored in CIT which is used during decryption procedure. The 2 shares are "XOR"ed to get the index of the color from CIT. Figure 2.13 (2015) shows the technique. Figure 2.13a and 2.13b shows binary share1 and share2 and 2.13c presents the recovered 256-color image having size same as original secret image.

2.3 Related work in the area of EVCTs

The technique proposed by Chang *et al.* (2000) is (2, 2)-EVCT for colored images in which two meaningful images (shares) called *camouflage images* are generated by embedding cover images into the shares. The secret image is hidden in the shares using cover images and a predefined table CIT. The dimensions of the cover images and the secret image are same. To get the secret image back from two camouflage images, one has to stack the images by performing logical "AND" operation along with the use of CIT. The technique is called *Modified Visual Cryptography*. The drawback of the technique is, when the number of colors in the secret image increases, the size of the CIT increases, so there is an overhead to store the table. Moreover, the technique is only 2-out-of-2 technique, as we increase the number of colors, the contrast of the recovered image decreases rapidly.

Ateniese *et al.* (2001) proposed the extension of VC which is EVC. EVCT generates meaningful shares rather than random noise-like shares in VC. The shares are made meaningful as share1 and share2 by embedding cover images. The cover images can be any non-secret images which are used to just give some meaning to the shares. Meaningful shares reduce the suspicion that something is concealed there. Researchers proposed (2, 2)-EVCT for binary images in which each white pixel from cover image is expanded to 2-white-2-black sub-pixel block and each black pixel from cover image is expanded to 1-white-3-black sub-pixel block in every share. When the shares are stacked, the resultant image would be having 1-white-3-black sub-pixel blocks corresponding to the white pixel of the original secret image and 4-black sub-pixel block corresponding to the black pixel of the original secret image. The shares have reduction in contrast by 50% while the regenerated original secret image has 75% contrast reduction.

The implementation for Ateniese's model is described here in which each pixel from original image is converted into 2×2 sub-pixel block. The technique produces the resultant secret

image with reduction in contrast. The shares in EVCT are made using black-and-white cover images and hence there is reduction in contrast of shares by 50%. In resultant image has 75% reduction in contrast. Figure 2.14 shows the technique. Figure 2.14a shows black-and-white original image, 2.14b and 2.14c shows black-and-white cover images, 2.14d and 2.14e shows corresponding shares generated, 2.14f shows resultant stacked image.

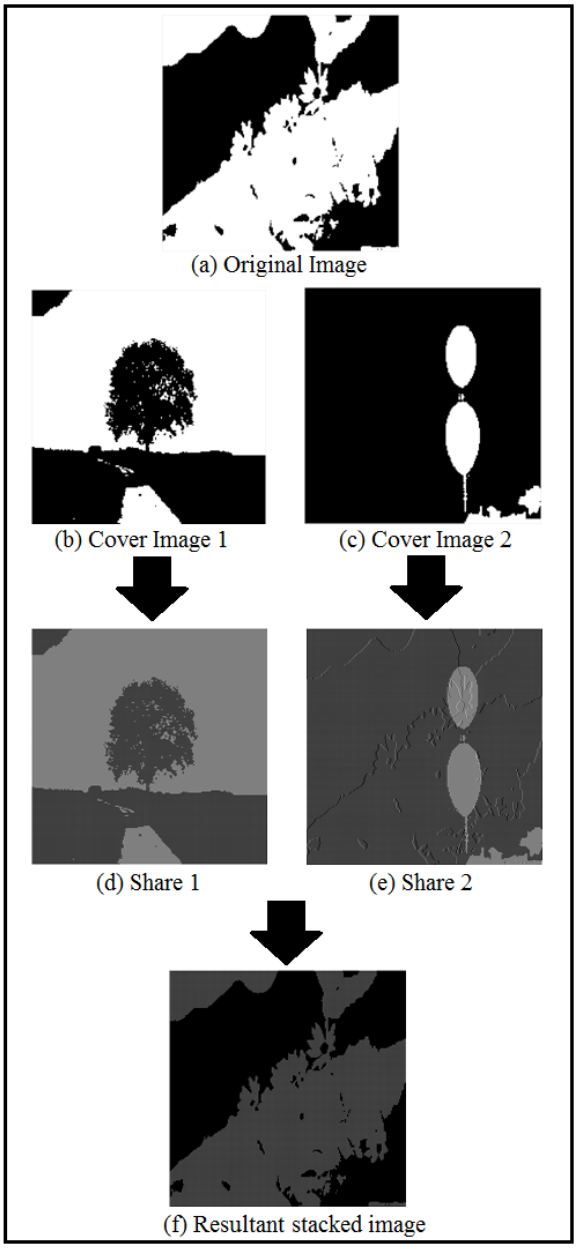


Figure 2.14: EVCT for black-and-white image

Hwang and Chang (2001) customized Ateniese's EVCT model by taking each pixel from original image as 3×3 sub-pixels block in share images. The shares are having 5 black

sub-pixels out of total 9 sub-pixels if the color of the pixel in the cover image is white and 7 black sub-pixels if the color of the pixel in the cover image is black. The regenerated image would be having 7 black sub-pixels if the color of the pixel in the original image is white and 9 black sub-pixels if the color of the pixel in the original image is black.

The technique proposed by Chang and Yu (2002) is (n, n)-Colored EVCT. The secret image consists of 256 colors. Each pixel in the original secret image is expanded to 9 sub-pixels in each of the n shares. The structure is described by a matrix S_{ij} and $[S_{ij}]$=1 when jth sub-pixel in the ith share is a non-white pixel where $1 \leq i \leq n$ and $1 \leq j \leq 9$. The operation used for decrypting the original secret image is "XOR" logical operation. Researchers proposed a uniform 2-out-of-2 scheme and then a general n-out-of-n scheme.

Nakajima and Yamaguchi (2002) proposed a new EVCT by making binary meaningful shares. In the technique, three natural images with intermediate gray-levels are given as input to the system and two images corresponding to the two input images are generated as output. These images are printed on transparencies and are stacked to produce the third image. The technique is implemented by using halftoning with Non-Periodic and Dot-Dispersed Dithering Algorithm. Authors also proposed the contrast improvement for enhancing the visual quality of the generated image in this paper.

Prakash and Govindraju (2007) proposed the Halftoned EVCT, as shown in Figure 2.15, by making n meaningful colored halftoned shares which are in Figure 2.15c and 2.15d. For making shares, two color images are required as shown in Figure 2.15a and 2.15b. The shares are having high quality with much less noise. The original image can be reconstructed by overlaying the shares onto one another without any computational complexity as shown in Figure 2.15e.

(a) Color image1 (b) Color image2 (c) Share1 (d) Share2 (e) Stacked result of Share1 and Share2

Figure 2.15: Halftoned EVCT

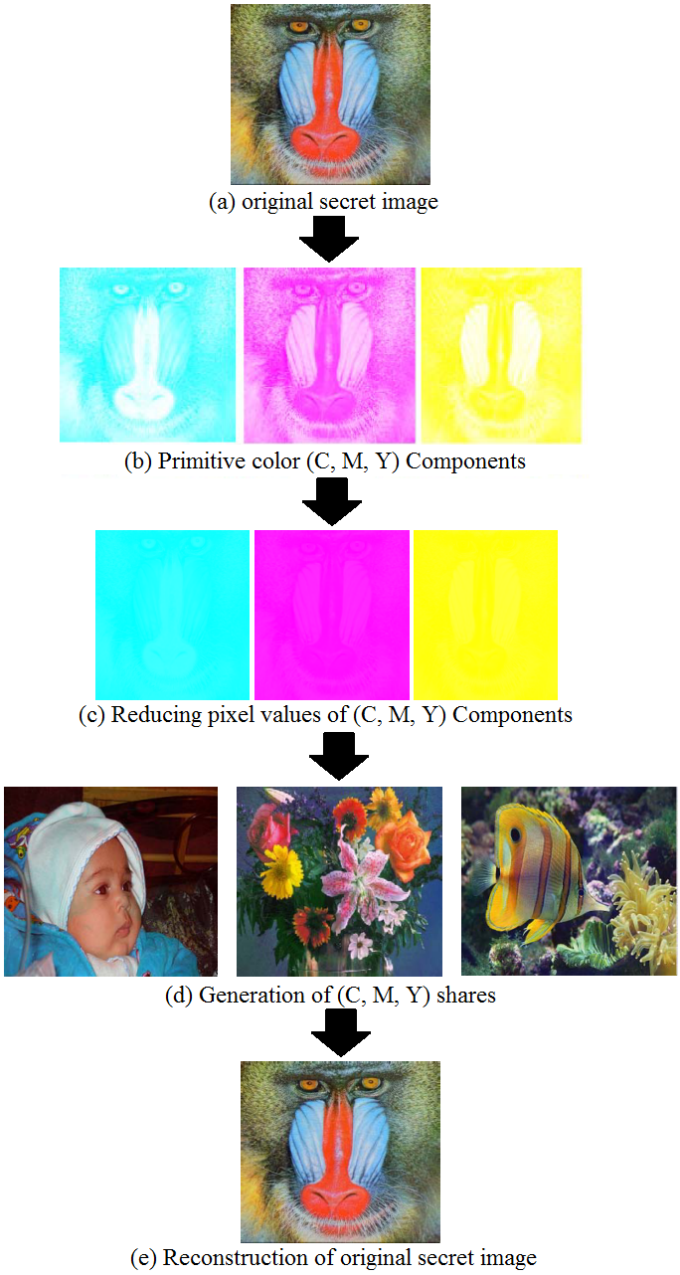


Figure 2.16: EVCT for true color (24 bits) secret image

Abdulla (2010) proposed an algorithm for EVCT for colored images. The algorithm takes four colored images as input and generates any three images which are mappings of the three input images. For decryption, any subset of the three images can be stacked to get the forth image. The size of the forth image will be same before and after encryption and decryption. The technique is implemented for true color images and all the generated shares are meaningful.

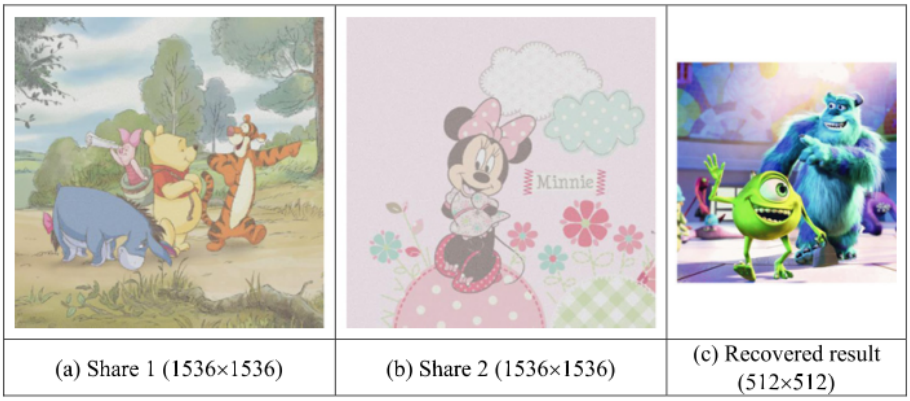


Figure 2.17: EVCT for 256-color secret image

For true color images (24-bit image), the original secret image as shown in Figure 2.16a is first converted into 3 primitive colors cyan, magenta and yellow as shown in Figure 2.16b. The three color images are then increased in intensity by one-forth as shown in Figure 2.16c. Three images are then merged with three cover images as shown in Figure 2.16d. The original image can be restored by stacking the three shares as shown in Figure 2.16e.

Liu and Wu (2011) proposed embedded EVCT for sharing black and white secret images. Two proposed techniques are (2, 2)-EVCT and (3, 3)-EVCT. Firstly, the shares are generated using VCT and then the gray-scale cover images are embedded into them to make the shares meaningful. The stacking of the shares would reveal the original secret image with reduced contrast.

Wei *et al.* (2015) proposed (2, 2)-EVCT using logical "XOR" and lossless (2, 2)-EVCT. The implementation for EVCT for 256 color secret image (8 bit image) and true color image (24 bit image) is discussed here. For 256-color secret images, the process of making meaningful shares is same as VCT for 256-color image but color of the cover image is filled in place of those 5 black pixels in both the shares. The cover images for both the shares are different. Figure 2.17 (2015) shows above technique. Figure 2.17a and 2.17b shows meaningful share1 and share2 with embedded cover images. Figure 2.17c shows the resultant 256-color image.

Chapter 3

Research Problem and Motivation

Chapter 2 discussed various ways to perform VCTs and EVCTs. This chapter focuses on the problem statement and motivation for proposing two new EVCTs for sharing a true RGB (24-bit) image.

3.1 Problem Statement

In the field of VC, an image is restored just by stacking the significant number of shares. This is not always the case, because some additional computations need to be done while sharing colored images. Increasing the number of colors in the secret image results in complex cryptographic procedure and more time to execute, which becomes less efficient in case of hard real time systems. In EVCT, meaningful shares are generated which is additional work to be done during encryption. The shares are made meaningful by embedding cover images into them and the effect of cover images has to be nullified during encryption of the secret image. This complete procedure needs additional computations and calculations which further increases the time to execute the procedures and space to store more amount of information. To share a black-and-white image, 1 bit/pixel is required to store the information and hence size of the shares would be less, storage space would be less and finally the transmission time of the shares would be less. To share a true RGB (24-bit) image, 24 bits/pixel is required to store the information and hence size of the shares would increase, storage space would increase and finally the transmission time would increase. So, there is a need to make a secure, simple, convenient and efficient techniques which keeps a trade-off between all the possible aspects of sharing a secret image.

3.2 Motivation of the Proposed Work

From the literature review, one can observe the drawbacks of the existing techniques. *(2, 3)*-threshold VCT proposed by Chao and Lin (2006) converts a 24-bit true colored image into a 3-bit image. So, the technique regenerates the secret image with reduced contrast. Although the technique is 2-out-of-3 VCT but an extra mask share is needed for decryption of the secret image. Shares generated are random noise-like shares. The technique proposed in (2003) for colored images have similar drawbacks as mentioned above in (2006). Moreover, the recovered secret image is the halftoned image instead of the continuous toned image. So, it would not be suitable to share the images with very high detailing like geographic maps.

In (2011), the proposed technique is only for gray scale images. The secret image can only be recovered from the qualified set of shares. Any threshold number of shares can't recover the secret image. Contrast of the recovered image is $1/9$ in (2, 2)-EVCT and $1/16$ in (3, 3)-EVCT. Good contrast is needed in images like medical images, spacial images. Moreover, the technique does not recover the secret image with complete resolution. So, the proposed technique would not be suitable for sharing such images.

In (2015), (2, 2)-EVCS technique is proposed for 256 colors to 65,536 colors and true color images using "XOR" operation. For sharing 256 to 65,536 colors image, a CIT is required to decrypt the secret image which means more the number of colors in the secret image, more will it take to decrypt the image because every time entire table would be scanned for each pixel. Along with this more memory would be required to store the table. Also, additional palette data is to be stored in the shares along with the pixel information because the bit is to be used in the algorithm. There is no proper algorithm mentioned for true color images. The proposed algorithm for sharing 256 colors to 65,536 colors images is based on palette bit data. The authors mentioned that there is no need to store the palette bit for true color images then how the algorithm can be applied to true color images. Moreover, the proposed technique used "XOR" instead of "OR", which is mostly used in conventional cryptographic schemes. Also there is no other variation of EVCT other than (2, 2)-EVCT in the paper. Contrast is comparatively less and the algorithm for sharing 256 colors is taking much time (207.8824 sec) to execute.

In (2017), (*k, n*)-CTVCS is proposed which uses halftoning concept to share the secret image. The generated shares are random noise-like shares. The shares are stacked to get the halftoned image and after that, a continuous tone image is generated by the halftoned image.

The recovered image is lossy.

3.3 Contribution of the Proposed Work

In order to remove the drawbacks of existing techniques, two techniques (3, 3)-EVCT and (2, 3)-EVCT have been proposed in this dissertation, for true color images without any data loss in the recovered secret image. No mask share is needed in decryption process of these proposed techniques as it was needed in (2003, 2006). Generated shares used in proposed techniques are meaningful thereby removing the drawback of the techniques proposed in (2003, 2006, 2017). There is no loss in the recovered image in the proposed techniques. Hence, these techniques can be applied to the images with high detailing like medical images, spacial images, maps. There is no need of CIT to decrypt the image. Hence the technique takes less time to implement which is about 3 sec for (3, 3)-EVCT and 5 sec for (2, 3)-EVCT for true color images which is much less than the time (207.8824 sec) taken by the technique in (2015) for 256 color images. The time taken by technique in (2015) for true color images would be even more. As there is no need to store the CIT table, hence less memory is required to implement the technique. Along with that no palette data is stored. The images generated by the proposed techniques have good contrast. Moreover these techniques use "OR" operation instead of "XOR" thereby removing all the drawbacks of the technique proposed in (2015). The recovered image is not the halftoned as in (2017) but continuous toned without any loss thereby removing the drawbacks of losslessness.

Chapter 4

Proposed Extended Visual Cryptography Techniques for Color Images

This chapter discusses the proposed techniques with encryption/decryption algorithms. Implementation results have also been presented in the chapter.

4.1 Basic Concept used in Proposed Techniques

In this work, two extended visual cryptography techniques for true color images are proposed. In first technique, (3, 3)-EVCT is proposed in which three RGB shares of a secret image are created. Out of these shares, first share contains R component, second contains G component and third contains B component of the secret image. All three shares are required to get the original secret image back on the receiver side. Second technique is (2, 3)-EVCT, in which any 2-out-of-3 shares are required to generate the original secret image. Out of these shares, first share contains the RG components, second contains GB components and third contains RB components of the input image. The generated shares are made meaningful in order to increase the security and to reduce the suspicion that something is hidden there. All shares in both the techniques are meaningful as they contain the cover images along with the information of the original secret image. The proposed techniques are lossless in nature and are less complex. The generated shares have block size of 5×5 corresponding to a pixel in original secret image. The dimensions of the original secret image, cover images, regenerated secret image are same.

8 bits each of R, G and B colors can be filled in a 5×5 block in such a way that if a position contains one color, then its immediate horizontal and vertical neighbors do not resemble the same color. But those positions can have other 2 colors. This concept is taken

to increase the distribution of 8 bits of each color as much as possible. This would increase the contrast of the shares. Also the images used for implementation are shown in Figure 4.1.

B_7	G_5	R_4	B_2	X
R_7	B_5	G_3	R_2	B_0
G_7	R_6	B_4	G_2	R_1
B_6	G_4	R_3	B_1	G_0
G_6	R_5	B_3	G_1	R_0

(a) 5×5 block showing the positions of each of 8 bits of R, G and B components including one left out position

```
If bit of any color component is 1:
    take bit color black
else:
    take bit color dark gray
```

(b) Color scheme for bit 1 and bit 0 in *RGB* components

Figure 4.1: 5×5 block used in shares and color scheme for component bits

4.2 Proposed (3, 3)-EVC Technique

As shown in Figure 4.2a, three RGB shares (R share, B share and G share) for (3, 3)-EVCT are generated using RGB color decomposition. Then, the meaningful cover images are embedded into the shares to make them meaningful. Shares are now ready to be sent over any unsecure communication medium according to the decryption procedure shown in Figure 4.2b, the effect of cover images is nullified from the three RGB shares. The shares are then overlapped to get a matrix. The matrix is then used to get the original secret image back.

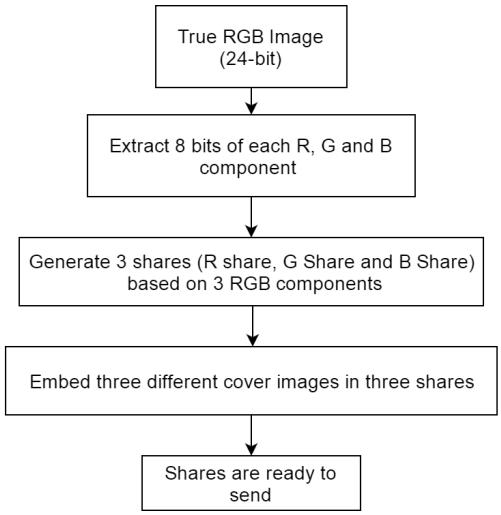
4.2.1 Encryption Algorithm

Encryption algorithm used in (3, 3)-EVCT has the following steps which are also shown in Figure 4.3.

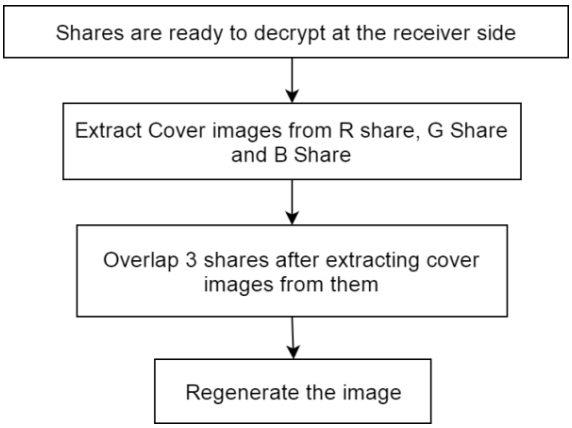
Step 1: Take a true colored RGB image (24 bits). Extract 8 bits each of R, G and B components of (i, j)th secret pixel.

Step 2: Expand the (i, j)th secret pixel of the original image to a 5×5 block in R share, G share and B share.

Step 3: Fill 8 bits each of R, G and B component in the corresponding R, G and B shares at specified positions of a 5×5 block as shown in Figure 4.1a. Fill the color of each bit in the shares. If bit is 1, fill black color at that position and if bit is 0, fill dark gray



(a) (3, 3)-EVCT Encryption Procedure



(b) (3, 3)-EVCT Decryption Procedure

Figure 4.2: Proposed (3, 3)-EVCT procedure

color as shown in Figure 4.1b. This way 24 out of total 25 positions of the 5×5 block would be in use. Leave one position as it is.

Step 4: Embed cover images into the shares. Fill the color of the (i, j)th pixel of cover image1, cover image2 and cover image3 into empty positions in R share, G share and B share respectively. Take three different cover images having same dimensions compared to the original secret image.

Step 5: Repeat steps 2-4, until every pixel of the original secret image is processed.

4.2.2 Decryption Algorithm

Decryption algorithm used in (3, 3)-EVCT decryption is illustrated in Figure 4.4.

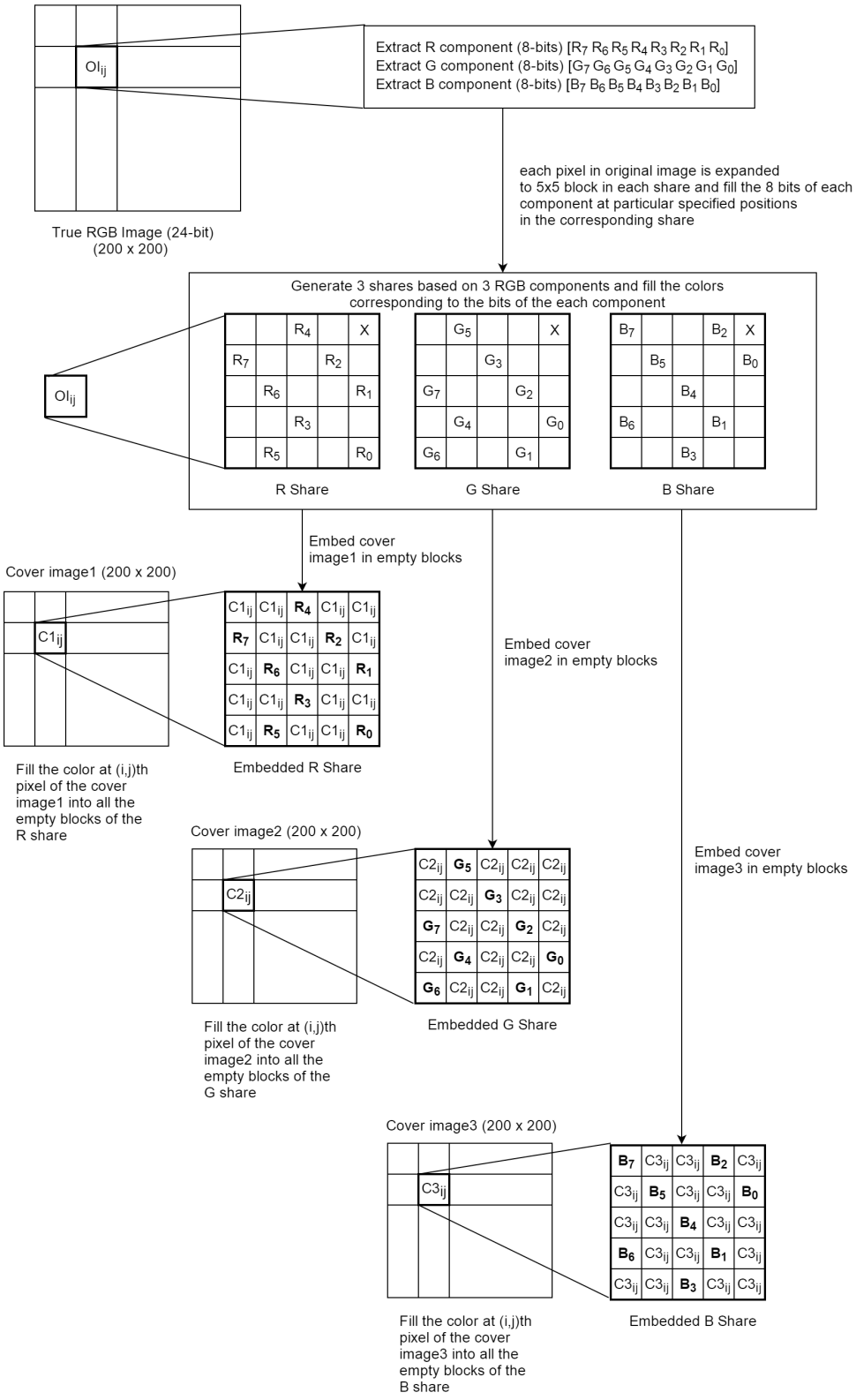


Figure 4.3: Steps of (3, 3)-EVCT encryption procedure in detail

Step 1: Take 3 meaningful shares embedded with cover images sent from the sender side.

Step 2: For each (i, j)th 5×5 block in each share, fill the positions which are having the colors of the cover images with zeros.

Step 3: The shares are now overlaid/superimposed by performing logical "OR" operation. The resultant share would be a matrix containing information about the 3 RGB components (in 5×5 block) for each pixel in the original secret image.

Step 4: Now the secret image can be regenerated from the matrix generated in the above step by taking 8 bits of each component from the specified positions as mentioned in Figure 4.1a.

4.3 Proposed (2, 3)-EVC Technique

The procedure for (2, 3)-EVCT is similar to (3, 3)-EVCT as shown in Figure 4.5a. The difference is in generating the shares. Every share would contain the information about any two out of three components. Hence RG, GB and RB shares would be created instead of R, G and B shares. As a result, any 2 shares would be able to generate the original secret image. Figure 4.5b shows the decryption procedure for (2, 3)-EVCT. Any two shares are selected to decrypt the image. The cover images are extracted from the shares and then two shares are overlapped to get the matrix. The secret image can be regenerated from the matrix.

4.3.1 Encryption Algorithm

(2, 3)-EVCT encryption algorithm has the following steps which are also illustrated in Figure 4.6.

Step 1: Take a true colored RGB image (24 bits). Extract 8 bits each of R, G and B components of (i, j)th secret pixel.

Step 2: Expand the (i, j)th secret pixel of the original image to a 5×5 block in RG share, GB share and RB share.

Step 3: Fill 8 bits of R component and 8 bits of G component in RG share, 8 bits of G component and 8 bits of B component in GB share, 8 bits of R component and 8 bits of B component in RB share at specified positions of a 5×5 block which is shown in Figure 4.1a. Fill the color of each bit in the shares. If bit is 1, fill black color at that

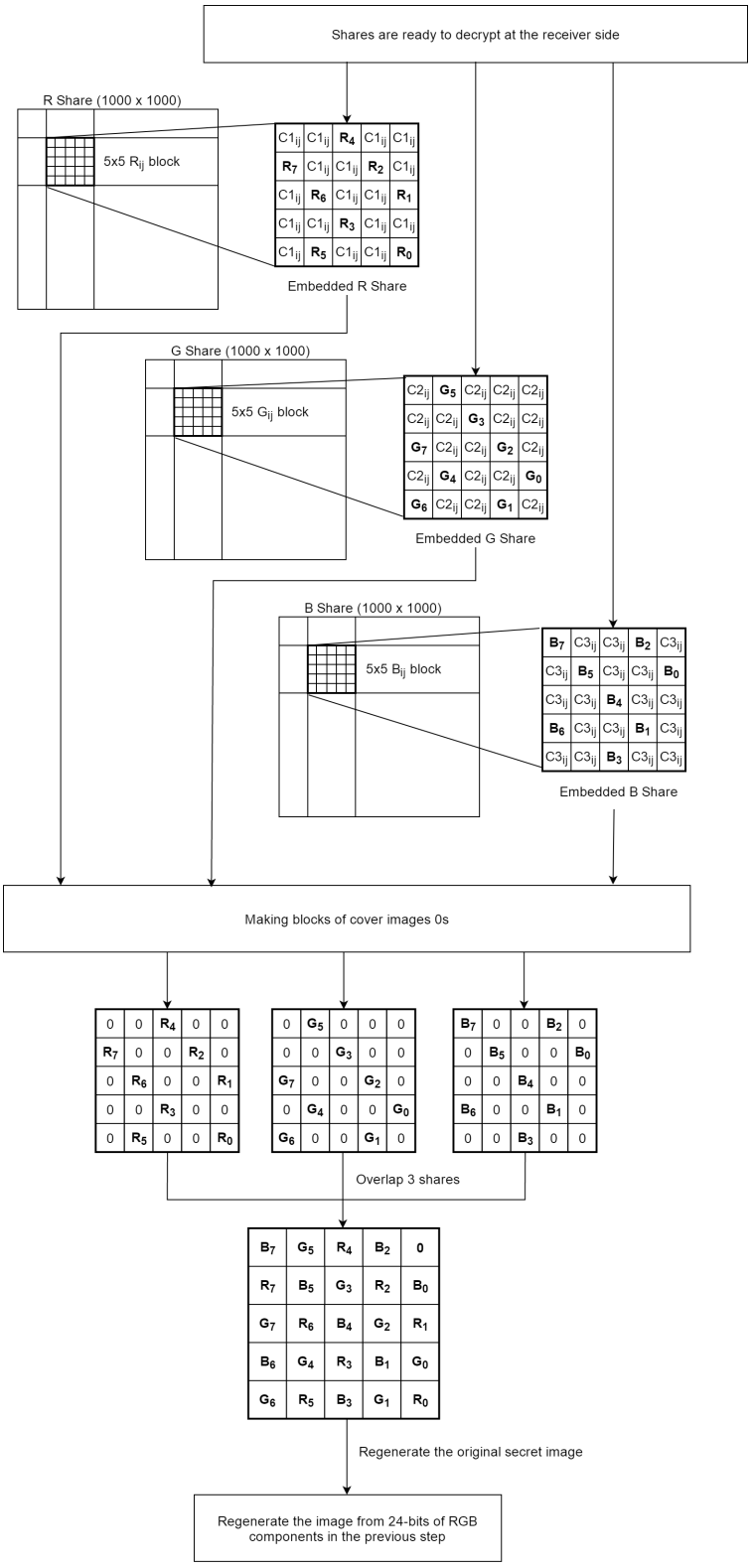
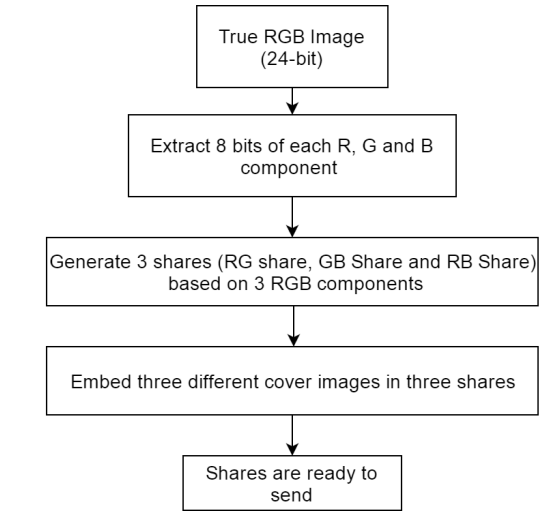
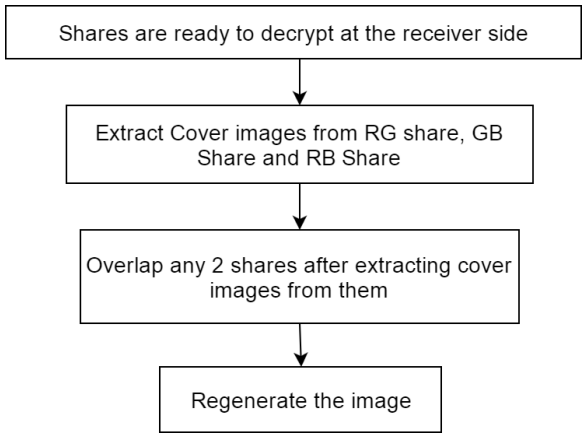


Figure 4.4: Steps of (3, 3)-EVCT decryption procedure in detail



(a) (2, 3)-EVCT Encryption Procedure



(b) (2, 3)-EVCT Decryption Procedure

Figure 4.5: Proposed (2, 3)-EVCT procedure

position and if bit is 0, fill dark gray color as shown in Figure 4.1b. This way 24 out of total 25 positions of the 5×5 block would be in use. Leave one position as it is.

Step 4: Embed cover images into the shares. Fill the color of the (i, j)th pixel of cover image1, cover image2 and cover image3 into empty positions in RG share, GB share and RB share respectively. Take three different cover images having same dimensions compared to the original secret image.

Step 5: Repeat steps 2-4, until every pixel of the original secret image is processed.

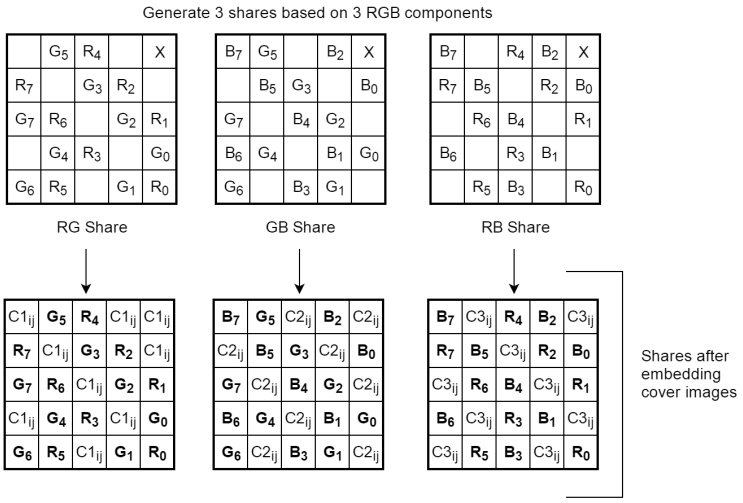


Figure 4.6: Steps of (2, 3)-EVCT encryption procedure in detail

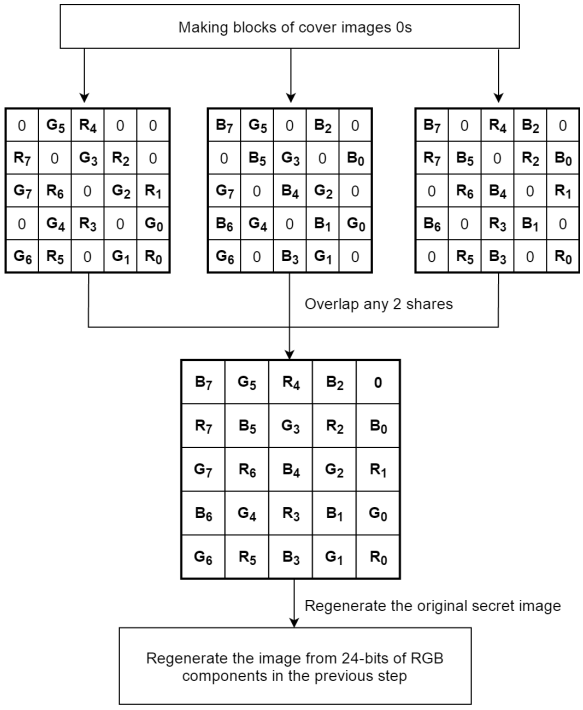


Figure 4.7: Steps of (2, 3)-EVCT decryption procedure in detail

4.3.2 Decryption Algorithm

Decryption Algorithm of (2, 3)-EVCT has the following steps which are also illustrated in Figure 4.7.

Step 1: Take any 2 meaningful shares embedded with cover images sent from the sender side.

Step 2: For each (i, j)th 5×5 block in each share, fill the positions which are having the colors

of the cover images with zeros.

Step 3: The shares are now overlaid/ superimposed by performing logical "OR" operation. The resultant share would be a matrix containing information about the 3 RGB components (in 5×5 block) for each pixel in the original secret image.

Step 4: Now the secret image can be regenerated from the matrix generated in the above step by taking 8 bits of each component from the specified positions as mentioned in Figure 4.1a.

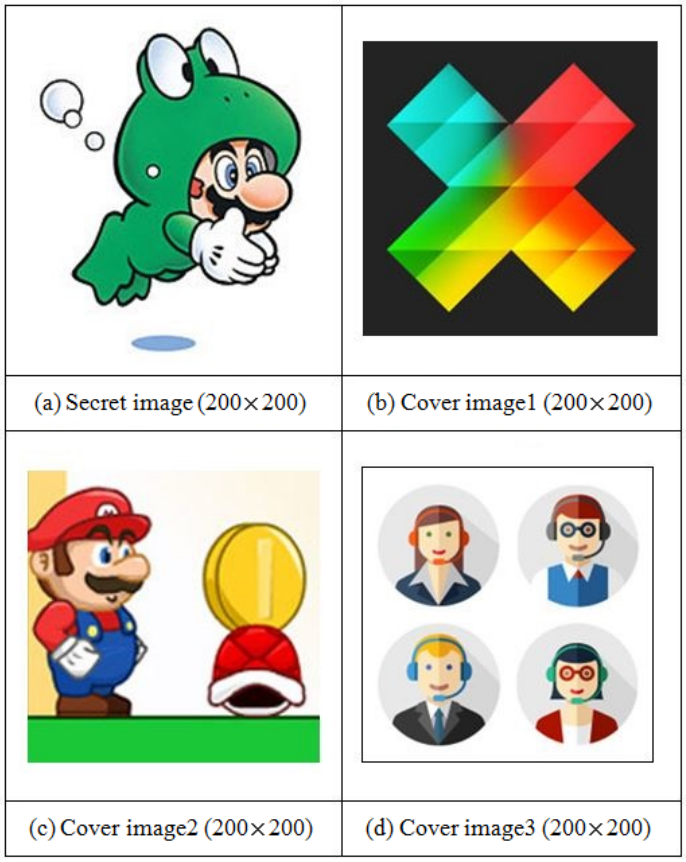
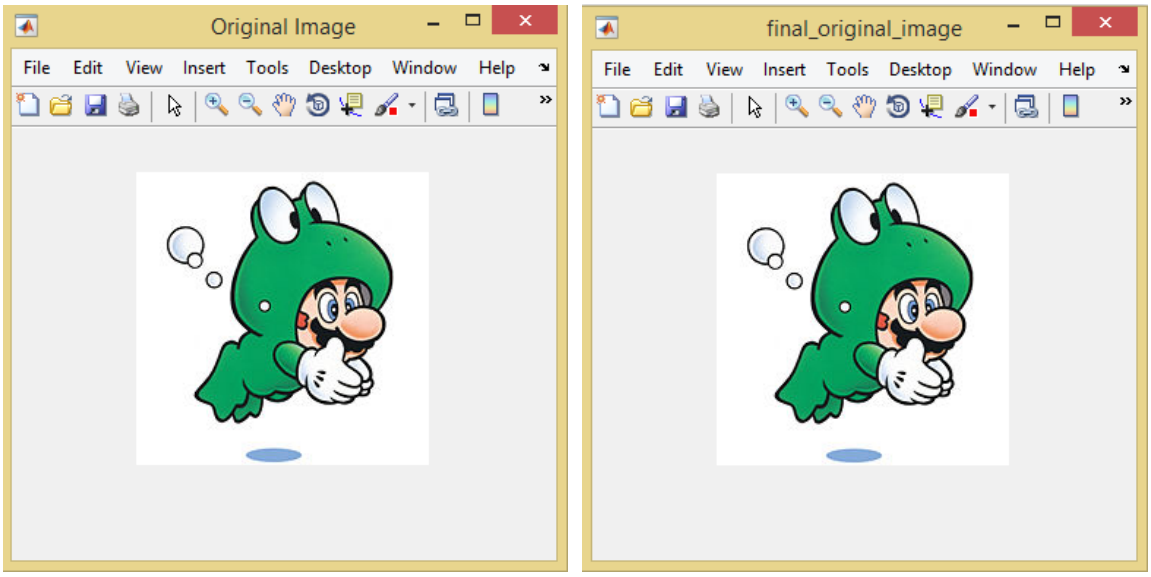


Figure 4.8: Test images used in implementation of Proposed Techniques

4.4 Experimental Results and Discussion

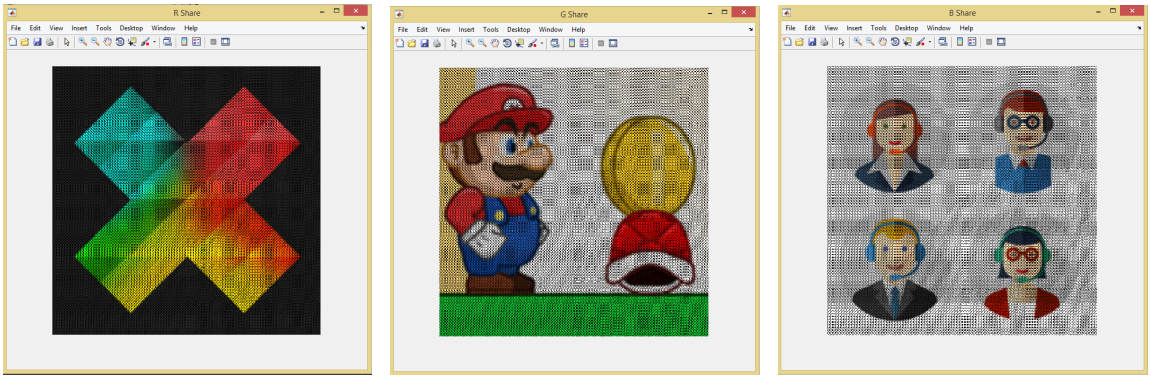
The original secret image, three cover images are random images having dimensions 200×200. All images are true RGB images. MATLAB R2016a is used for implementation of the techniques. The specifications of the machine which is used for implementation

purpose are Intel (R) Pentium (R) CPU N3540 @ 2.16 GHz with 4 GB RAM and 64-bits Windows operating system. All test images considered in experiments are presented in Figure 4.8.



(a) Original Secret Image (200×200) (b) Reconstructed Image (200×200)

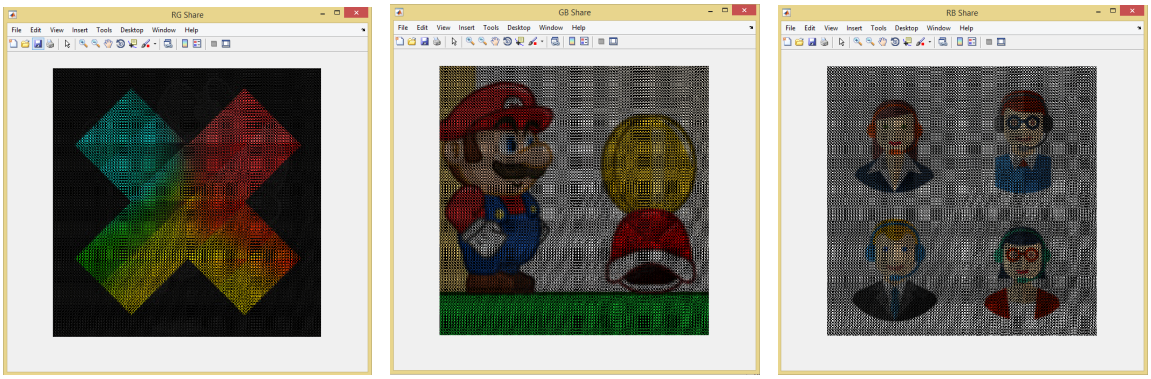
Figure 4.9: Original and reconstructed image



(a) R Share (1000×1000) (b) G Share (1000×1000) (c) B Share (1000×1000)

Figure 4.10: Three shares generated in (3, 3)-EVCT

The original secret image having dimensions 200×200 which is shown in Figure 4.9a. For (3, 3)-EVCT, R Share (1000×1000) is shown in Figure 4.10a, G Share (1000×1000) is shown in Figure 4.10b and B Share (1000×1000) is shown in Figure 4.10c. For (2, 3)-EVCT, RG Share (1000×1000) is shown in Figure 4.11a, GB Share is shown in Figure 4.11b and RB Share is shown in Figure 4.11c. The final reconstructed image is shown in Figure 4.9b



(a) RG Share (1000×1000) (b) GB Share (1000×1000) (c) RB Share (1000×1000)

Figure 4.11: Three shares generated in (3, 3)-EVCT

without any change in dimensions.

To show the effectiveness of the proposed techniques, the comparison with existing techniques is performed and this comparison is shown in Table 4.1. The comparison is done on the basis of the parameters given below:

i Pixel Expansion Ratio (m).

ii Total number of colors present in the original secret image.

iii Operations used for decrypting the secret image.

iv Nature of shares shows whether shares are random or meaningful.

v Losslessness of reconstructed image which shows that whether the recovered image is lossy or not.

Naor and Shamir (1995) technique shares the secret image with only two colors, that is, black and white by using pixel expansion in such a way that half of sub-pixels are taken as black and half are taken as white. The pixel expansion ratio can be 2, 4, 8 and so on. "OR" logical operation is used for decryption. The technique is lossy and generates random noise-like shares. Koga and Yamamotq (1998) proposed a lattice based VC which can share a secret image with J number of colors with pixel expansion of 2, 4, 8 and so on. The decryption is done by calculating the LUB of corresponding elements of two shares. The generated shares are random noise-like. Moreover, the technique is lossy in nature. Chang *et al.* (1999) technique uses 3×3 pixel expansion ratio to share a secret image having 5 colors only. The number of colors of the secret image is less. Now a days colored images

Table 4.1: Comparative analysis of various existing VCTs/EVCTs with the Proposed Techniques

	Pixel Expansion Ratio	**Colors**	**Operations**	**Nature of Shares**	**Resultant Image**
Naor and Shamir (1995)	2, 4, 8...	2 (binary)	"OR"	random	lossy
Verheul and Tilborg (1997)	b	c	"OR"	random	lossy
Koga and Yamamotq (1998)	2, 4, 8...	J	"OR" and LUB	random	lossy
Chang *et al.* (1999)	3×3	5	"AND"	random	lossless
Hofmeister *et al.* (2000)	$k \times k$	s	"AND" and CIT	meaningful	lossy
Lin (2000)	3×3	256	"AND"/"OR"	random	lossless
Ateniese (2001)	2×2	2 (binary)	"OR"	meaningful	lossy
Hou (2003)	2×2	256-gray scale and colored image	"OR"	random	lossless
Jin *et al.* (2005)	6×6	256 Halftone-image	Stacking Shares "XOR"	random	lossy
Chao and Lin (2006)	2×2	24-bit true RGB image	"OR" and a mask share	random	lossy
Klein and Wessler (2007)	Minimal	Gray scale image	"OR"	meaningful	lossy
Lou et al. (2007)	2	2 (binary)	"XOR"	random	lossy
Prakash and Govindraju (2007)	6	24-bit colored image	"OR"	meaningful	lossy
Kandar and Dhara (2011)	1	32-bit colored image including transparency component α	"OR"	random	lossy
Liu and Wu (2011)	3×3	2 (binary)	"OR"	meaningful	lossy
Prisco and Santis (2013)	$\lceil \log_3 n \rceil$	2 (binary)	"OR"	colored random	lossy
Gurung *et al.* (2014)	1	2 (binary)	"OR"	random	lossless
Lou *et al.* (2014)	3	24-bit colored image	"OR" and a secret key	random	lossy
Pooja and Lalitha (2014)	1	256-gray scale and colored images	Computer support	random	lossy
Wei *et al.* (2015)	3×3, 4×4, 5×5	256 colored , 65,536 colored and 24 bit true RGB image	"XOR" and CIT	random and meaningful both	lossless
Proposed Techniques	5×5	24-bit true RGB image	"OR"	meaningful	lossless

are more in use than the images with fewer colors. Chang *et al.* (2000) proposed EVCT for sharing a color image having *s* colors. Pixel expansion ratio is k×k. As the number of colors in the secret image increases, contrast of the recovered image decreases rapidly and size of CIT increases. Logical "AND" operation and CIT is used for decryption. The shares are meaningful and the technique is lossy in nature.

Lin (2000) proposed a technique in which a secret image with 256 colors can be shared by using logical "AND"/"OR" operations. Also the technique uses a mask share to enhance the security of noise-like shares. Ateniese (2001) proposed EVCT for binary images. The technique used 2×2 block as pixel expansion ratio that means the shares are 4 times larger than the original secret image. The reconstructed image in lossy in nature. Hou [2003] shared 256-gray scale and colored image with pixel expansion ratio of 2×2. The technique generates random noise-like shares. The decryption process is performed by logical "OR" operation and is lossy in nature.

Jin *et al.* (2005) proposed a technique to share a 256-color secret image using halftoning concept. The decryption is done by stacking the shares and performing logical "XOR" operation. The reconstructed image would be a 256-color halftone image. The limitation of the technique is that the pixel expansion ratio is 6×6 which is very high. The shares are 36 times larger than the original secret image which would take more memory space for storage and more time for transmission. Chao and Lin (2006) shared a 24-bit true RGB image with pixel expansion of 2×2. The size of shares are 4 times as compared to original secret image. Along with logical "OR" operation, a mask share is needed for decryption procedure which is a drawback of the technique. The shares are random noise-like and lossy in nature.

Prakash and Govingraju (2007) proposed EVCT for sharing 24-bit colored images with "OR" logical operation. The pixel expansion ratio is 6. The shares generated are meaningful and the technique generates lossy reconstructed image. Kandar and Dhara (2011) shared a 32-bit image which included α component in it for transparency. The pixel expansion ratio is 1 that means the size of the shares is same as the original image. The shares are random and the decryption process is lossy in nature. Liu and Wu (2011) proposed the similar technique but with higher pixel expansion. Each pixel from original secret image is expanded to 3×3 block which means the shares are 9 times larger than the original secret image.

Gurung *et al.* (2014) kept the size of the shares equal to the size of the original secret

image by taking pixel expansion ratio 1. They shared black-and-white secret image using "OR" operation and generated random noise-like shares without any loss in the reconstructed image. Lou *et al.* (2014) proposed a technique for sharing a 24-bit colored image using halftoning with pixel expansion ratio of 3. The disadvantage of the technique is that it uses secret key along with stacking the shares. The technique generates random noise-like shares and is lossy in nature. Pooja and Lalitha (2014) proposed a VCT for sharing 256-gray scale or colored images without any pixel expansion. The decryption is done using computer support. The generated shares are random and technique reconstructs lossy image.

Wei *et al.* (2015) proposed a technique to share an image having colors from 256 to 65,536 and a true color image using "XOR" operation. The pixel expansion ratio varies as the number of colors in the secret image increases. The technique is limited to (2, 2)-EVCT. The secret image in the proposed techniques can be generated either by stacking three shares in first technique or by stacking any two shares in second technique using logical "OR" operation. The shares are meaningful. Moreover, the proposed techniques are for sharing a true color RGB secret image and generates lossless image.

Chapter 5

Conclusion and Future Scope

This chapter describes conclusion and the future scope of the work presented in the dissertation.

5.1 Conclusion

In this dissertation work, Two EVCT techniques for digital images are proposed which generate meaningful shares. These techniques are (3, 3)-EVCT and (2, 3)-EVCT. The dimensions of the secret, cover and reconstructed images are same.

In (3, 3)-EVCT, three RGB components of every pixel in a true colored secret image is extracted. Three shares are generated, that is, R share, G share and B share. Each 8 bits of RGB components are stored in corresponding shares. The three shares should be filled with three different cover images. In this way three meaningful shares are generated. In (2, 3)-EVCT, three RGB components of every pixel in a true colored secret image is extracted. Three shares are generated, that is, RG share, GB share and RB share. RG share would contain the information about R and G components, GB share would contain the information about G and B components, RB share would contain the information about R and B components. In (3, 3)-EVCT, decryption can be done just by overlapping the three shares and extract the 24 bits of each pixel and the secret image can be regenerated. In (2, 3)-EVCT, decryption can be done just by overlapping any 2-out-of-3 shares and extract the 24-bits of each pixel and the secret image can be regenerated.

Any high detailed secret image can be shared with the proposed techniques without any loss of information and visual quality of the reconstructed image. Encryption and decryption procedures are convenient and simple to execute. The secret image used in this paper for

experimental purpose is having dimensions 200×200. Results of the proposed techniques with images having high dimensions can be analyzed. High dimensional images include medical images, geographic maps, spacial images, satellite images and so on. These images have large number of colors and have high number of pixels. Hence, proposed techniques can be suitable way to share these kind of images with security and efficiency. Moreover, the techniques take less time to implement which adds benefit for real time systems. The techniques with delays are not suitable for real time systems.

5.2 Future Scope

The proposed techniques are limited to (3, 3)-EVCT and (2, 3)-EVCT. These techniques can be extended to general (k, n)-EVCT or (n, n)-EVCT to increase the security. As each pixel from the original secret image is converted into 5×5 block which is costly from memory point of view because it increases the size of the shares. So, the methodology can be established to decrease size of the shares which would further decrease memory requirement and the transmission time of the shares. Also, only one secret image can be shared at a time with one time execution of the technique. Work can be done to increase the number of secret images shared at a time.

Bibliography

[1] Ateniese G., Blundo C., De Santis A., and Stinson D. R., "Extended capabilities for visual cryptography," Theor. Comput. Sci., vol. 250, no. 1-2, pp. 143-161, 2001.

[2] Abdulla S., "New Visual Cryptography Algorithm For Colored Image," J. Comput., vol. 2, no. 4, pp. 2151-9617, 2010.

[3] Chang C. C., Tsai C. S. and Chen T.S., "A technique for sharing a secret color image," Proc. of 9th National Conference of Information security, pp. LXIII-LXXII, 1999.

[4] Chang C., Tsai C., and Chen T., "A new scheme for sharing secret color images in computer network," Proceedings of International Conference on Parallel and Distributed Systems, pp. 21-27, 2000.

[5] Chang C. C., and Yu T. X., "Sharing a Secret Gray Image in Multiple Images," Proceedings of International Symposium on Cyber Worlds: Theories and Practice, Tokyo, Japan, pp. 230-237, 2002.

[6] Chao K. and Lin J., "(2 , 3) -Threshold Visual Cryptography for Color Images Cryptography," Proceedings of the 6th WSEAS International Conference on Signal Processing, vol. 2006, pp. 89-94, 2006.

[7] De Prisco R. and De Santis A., "Color visual cryptography schemes for black and white secret images," Theor. Comput. Sci., vol. 510, pp. 62-86, 2013.

[8] Gurung S. and Ojha G., "Multiple Image Encryption using Random Circular Grids and Recursive Image Hiding," International Journal of Computer Applications, Taichung, vol. 86, no. 10, pp. 19-24, 2014.

[9] Hofmeister T., Krause M., and Simon H. U., "Contrast-optimal out of secret sharing schemes in visual cryptography," Theor. Comput. Sci., vol. 240, no. 2, pp. 471-485, 2000.

[10] Hwang R. J., Chang C. C., “Hiding a picture in two pictures,” Opt. Eng., vol. 40, pp. 342-351, 2001.

[11] Hou Y., “Visual cryptography for color images,” Pattern Recognition, vol. 36, pp. 1619-1629, 2003.

[12] Jin D., Yan W. Q., Kankanhalli M. S., “Progressive color visual cryptography”, J. Electron. Imaging, vol. 14, no. 3, pp. 033019-1-033019-13, 2005.

[13] Koga H. and Yamamotq H., “Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E81-A, no. 6. pp. 1262-1269, 1998.

[14] Klein A. and Wessler M., “Extended visual cryptography schemes,” Inf. Comput., vol. 205, no. 5, pp. 716-732, 2007.

[15] Kandar S. and Dhara B. C., “k-n Secret Sharing Visual Cryptography Scheme on Color Image using Random Sequence,” International Journal of Computer Applications, vol. 25, no. 11, pp. 6-11, 2011.

[16] Karolin M. and Meyyapan T., “RGB Based Secret Sharing Scheme in Color Visual Cryptography,” vol. 4, no. 7, pp. 151-155, 2015.

[17] Lin F., “A New Approach on Color Secret Image Sharing Technique”, Department of Information Management, National Central University, 2000.

[18] Lou D. C., Tso H. K., and Liu J. L., “A copyright protection scheme for digital images using visual cryptography technique,” Comput. Stand. Interfaces, vol. 29, no. 1, pp. 125-131, 2007.

[19] Liu F. and Wu C., “Embedded Extended Visual Cryptography Schemes,” IEEE transactions on information forensics and security, vol. 6, no. 2, pp. 307-322, 2011.

[20] Lee C. C., Chen H. H., Liu H. T., Chen G. W., and Tsai C. S., “A new visual cryptography with multi-level encoding,” J. Vis. Lang. Comput., vol. 25, no. 3, pp. 243-250, 2014.

[21] Luo H., Chen H., Shang Y., Zhao Z., “Color transfer in visual cryptography,”Measurement, vol. 51, pp. 81-90, 2014.

[22] Lalitha Y. S., “Non Expanded Visual Cryptography for Color Images using Pseudo Randomized Authentication,” International Journal of Engineering Research and Development, vol. 10, no. 6, pp. 1-8, 2014.

[23] Noar M. and Shamir A., “Visual Cryptography,” Adv. Cryptogr., pp. 1-12, 1995.

[24] Nakajima M. and Yamaguchi Y., “Extended Visual Cryptography for Natural Images”, 2002.

[25] Prakash N. K. and Govindaraju S., “Visual Secret Sharing Schemes for Color Images using Halftoning,” International Conference on Computational Intelligence and Multimedia Applications, pp. 174-178, 2007.

[26] Sreekumar A., “Secret sharing schemes using visual cryptography,” vol. 95, pp. 90-95, 2009.

[27] Verheul E. and Tilborg H. V., “Constructions and properties of k out of n visual secret sharing schemes,” Designs, Codes and Cryptography, pp. 179-196, 1997.

[28] Weir J. and Yan W., “Visual Cryptography and its Applications”, 2012.

[29] Wei S. C., Hou Y. C., and Lu Y. C., “A technique for sharing a digital image,” Comput. Stand. Interfaces, vol. 40, pp. 53-61, 2015.

[30] Yang C. N., Tung T. C., Wu F. H., and Zhou Z., “Color transfer visual cryptography with perfect security,” Measurement, vol. 95, pp. 480-493, 2017.

List of Publications

[1] **Kirti Dhiman**, Singara Singh Kasana and Harkiran Kaur, "Extended Visual Cryptography Techniques for True Color Images", Computers and Electrical Engineering, SCI Elsevier Journal. **[Under Revision]**

[2] **Kirti Dhiman**, Harkiran Kaur and Singara Singh Kasana, "VCT and EVCT for black-&-white and Colored Images", 2nd International Conference on Advanced Computing and Intelligent Engineering (ICACIE 2017), 2017. **[Communicated]**

Video Presentation Link

https://www.youtube.com/watch?v=2IEsFNj5NEs