DEVELOPMENT OF COPYRIGHT PROTECTION AND AUTHENTICATION SCHEMES WITH EXTENDED VISUAL CRYPTOGRAPHY

THESIS SUBMITTED

FOR THE AWARD OF DEGREE OF

DOCTOR OF PHILOSOPHY

BY

SONAL KUKREJA
REGISTRATION NO. 901603018

UNDER THE GUIDANCE OF

DR. SINGARA SINGH KASANA
ASSOCIATE PROFESSOR

DR. GEETA KASANA
ASSISTANT PROFESSOR

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR INSTITUTE OF ENGINEERING AND TECHNOLOGY
PATIALA, PUNJAB, INDIA-147004
SEPTEMBER 2020

CERTIFICATE

I hereby declare that the work being presented in this thesis titled as **Development of Copyright Protection and Authentication Schemes with Extended Visual Cryptography**, in fulfillment of the requirements for the award of degree of **DOCTOR OF PHILOSOPHY** submitted in Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Singara Singh Kasana, Associate Professor, Computer Science and Engineering Department and Dr. Geeta Kasana, Assistant Professor, Computer Science and Engineering Department and refers other researcher works, which are properly referenced.

This thesis's content has not been submitted for the award of any other degree at this or any other University.

(**Sonal Kukreja**)

Registration No. 901603018

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

(**Dr. Singara Singh Kasana**)

Associate Professor, CSED

TIET, Patiala

Supervisor

(**Dr. Geeta Kasana**)

Assistant Professor CSED

TIET, Patiala

Supervisor

Acknowledgements

Undertaking this Ph.D. has been a truly life-changing experience for me and I would not have been able to complete it without the assistance and guidance of many people.

I would like to express my sincere gratitude to my supervisors, **Dr. Singara Singh Kasana** and **Dr. Geeta Kasana**, for their consistent support, encouragement and immense knowledge. I am highly indebted to them for their invaluable time and effort they invested in me throughout my research journey. Their guidance and patience helped me in carrying out conduct by research effectively.

I am thankful to my Ph.D. committee which includes **Dr. Maninder Singh**, Professor and Head, **Dr. Sanmeet Bhatia**, Associate Professor, **Dr. Shreelekha Pandey**, Assistant Professor, Computer Science and Engineering Department and **Dr. Kulbir Singh**, Professor, Electronics and Communication Engineering Department, for keeping track of my progress and giving helpful suggestions to improve my work. I thank the entire faculty and staff of Computer Science and Engineering Department for their support and cooperation.

I would like to express my gratitude to my loving parents, **Dr. Ravi Kukreja** and **Indra Kukreja**, for believing in me and motivating me to pursue my goals.Finally, I want to thank my sister, Meenal Kukreja, and my husband, Dikshit Bhardwaj, for always being there for me and supporting me to keep going. Last but not least, I would like to thank God for providing me the courage, the wisdom, the ability and the opportunity to pursue and complete this research. Without his blessings, this success would not have been possible.

(**Sonal Kukreja**)

Abstract

The existing image watermarking schemes protect the digital image by embedding watermark that degrades the visual quality of the image. This embedded watermark is extracted to prove the copyright or authentication. Visual Cryptography based watermarking schemes have gained a lot of attention in recent years since they aid in protecting the images without modifying them. The focus of this thesis is on two key uses of watermarking, namely copyright protection and authentication.

Most of the existing Visual Cryptography based image authentication schemes have high computational cost as they embed the constructed shares and authentication data into the cover images. Most of these schemes create expanded and noisy shares, leading to pixel expansion and security threat of some sensitive information being shared, respectively. To address these problems, an imperceptible authentication scheme is introduced for grey images where meaningful and un-expanded authentication shares are generated from watermark and cover images. Cellular Automata is used to construct the master share that provides self-construction capacity to the share, thereby saving the storage cost and enhancing stability. The watermark is recovered just by superimposing these authentication shares, thereby helping to reduce the computational cost at receiver's side. The scheme possesses the ability of tamper detection, localization and lossless recovery as of the tampered data as well.

The copyright protection schemes are proposed to protect the ownership of the digital images. Most of the existing copyright protection schemes based on visual cryptography produce noisy shares that is a security threat. For this purpose, a robust and secure copyright protection scheme based on curvelet transform, K-means clustering and extended visual cryptography for color images is proposed that creates meaningful noiseless shares. The scheme is robust to withstand a

range of image manipulation attacks and provide greater imperceptibility. The effectiveness of the scheme is shown by comparing it with existing copyright protection schemes. However this scheme was unable to handle false positive cases, where the false owners can also prove their copyright on the image. As a result, this scheme has been enhanced to cope successfully with false positive scenarios by using two watermarks. One of them is provided by the user and the other is created from the host image. The latter is used to cope with false positives as it contains the host image information. This scheme works only for single images with single owners. As a result, this scheme was further extended to multiple images and multiple owners.

To the best of our knowledge, two copyright protection schemes (Amiri and Moghaddam (2016), Liu and Wu (2011)) exist in the literature, for multiple images. These schemes have some limitations like meaningless shares, false positives and side information transmission. In addition, these schemes involve the presence of every ownership share to prove the copyright. This limits the schemes, as if any of these ownership shares are not accessible, the other owners can not prove their copyright. To fix these concerns, a robust copyright protection scheme for multiple color images with multiple owners is proposed that creates meaningful shares where a qualified set of owners can verify the ownership. Three types of shares are included in this scheme: *i.e.* master share, ownership share and key share. The ownership share is generated using a master share and a watermark that is then used to construct a key share that is stored with the Trusting Authority. To prove the copyright of multiple images, the ownership shares and the key share are superimposed to retrieve the watermark. The visual appearance of the watermark proves the copyright of rightful owners.

Experimental results demonstrate the efficiency of the proposed schemes. Comparisons with existing Visual Cryptography based watermarking schemes show improved performance of the proposed schemes.

Abbreviations

AS	Authentication Share
BER	Bit Error Rate
CA	Cellular Automata
CRT	Chinese Remainder Theorem
DWT	Discrete Wavelet Transform
DCT	Discrete Cosine Transform
DCuT	Discrete Curvelet Transform
DR	Detection Ratio
EVCS	Extended Visual Cryptography Scheme
FFT	Fast Fourier Transform
FrFT	Fractional Fourier Transform
GF	Galois Field
HVS	Human Visual System
LBP	Local Binary Pattern
LSB	Least Significant Bit
MS	Master Share
MSE	Mean Square Error
NHS	Normalized Hamming Similarity
NC	Normalized Correlation
OS	Ownership Share
PRNG	Pseudo Random Number Generataor
PSNR	Peak Signal to Noise Ratio
SDM	Sampling Distribution of Means
SIFT	Scale Invariant Feature Transform
SIS	Secret Image Sharing
SIVCS	Size Invariant Visual Cryptography Scheme

SSIM	Structural Similarity Index
SURF	Speeded Up Robust Features
SVD	Singular Value Decomposition
TA	Trusting Authority
TAF	Tamper Assessment Function
VC	Visual Cryptography
XOR	Exclusive-OR
WPD	Wavelet Packet Decomposition
WRAP	Frequency Wrapping

Notations and Symbols

Symbol	Meaning
I	Image
$N \times N$	Image size
(x, y)	Image Pixel
n	Number of Participants
k	Minimum number of participants required for superimposition
m	Pixel Expansion rate
Z_0	Set of matrices for meaningless share construction for white pixel
Z_1	Set of matrices for meaningless share construction for black pixel
C_0	Set of matrices for meaningful share construction for white pixel
C_1	Set of matrices for meaningful share construction for black pixel
τ_{qual}	Set of qualified shares
τ_{forb}	Set of forbidden shares
K	Number of clusters in K-means Clustering
nb	Number of Blocks
HI	Host Image
$hh \times hw$	Host Image Size
HI'	Received Host Image
CI	Cover Image
$ch \times cw$	Cover Image Size
WI	Watermark Image

$wh \times ww$	Watermark Image Size
w	Watermark bit
W'	Extracted Watermark Image
W_2	Self Constructed Watermark
$CI(x,y)$	Cover Image pixel
$SI(x,y)$	Stego Image pixel
CI_{bit}	Cover Image bit
W_{bit}	Watermark bit
M	Binary representation matrix for decimal numbers
$M_{c,d}$	Codebook Matrix
Map	Binary Matrix
$mh \times mw$	Size of Map
$b_{i,j}$	block at i^{th} row and j^{th} column
$nh \times nw$	Size of Image in terms of Blocks
C_i	Concatenated transformed and scrambled matrix
HI_b	Host Image Block
CI_b	Cover Image Block
MS_b	Master Share Image Block
WI_b	Watermark Image Block
MM	Master Feature Matrix
Avg_b	Mean of the block pixels
p	probability
Q	JPEG Compression quality factor
θ	Rotation angle
ws	Medan Filtering window size
cw	Cropping window size
V	Variance
D	Noise density
R	Radius
A	Sharpening Amount

Contents

List of Figures

List of Tables

List of Publications

i. **Sonal Kukreja**, Geeta Kasana and Singara Singh Kasana, “Curvelet transform based robust copyright protection scheme for color images using extended visual cryptography", Multimedia Tools and Applications, Vol. 79, pp. 26155–26179, 2020, Impact Factor: 2.313.

ii. **Sonal Kukreja**, Geeta Kasana and Singara Singh Kasana, “Extended visual cryptography-based copyright protection scheme for multiple images and owners using LBP-SURF descriptors", The Visual Computer, 2020, https://doi.org/10.1007/s00371-020-01883-9, Impact Factor: 1.456.

iii. **Sonal Kukreja**, Geeta Kasana and Singara Singh Kasana, “Cellular Automata based Image Authentication Scheme using Extended Visual Cryptography", Computing and Informatics, Vol. 38, pp. 1272-1300, 2019, Impact Factor: 0.574.

iv. **Sonal Kukreja**, Geeta Kasana and Singara Singh Kasana, “Copyright Protection Scheme for Color Images with Meaningful Shares", Computers and Electrical Engineering, Vol. 91, 2021, https://doi.org/10.1016/j.compeleceng.2020.106931, Impact Factor: 2.663.

v. **Sonal Kukreja**, Geeta Kasana, and Singara Singh Kasana, “Visual cryptography based robust copyright protection scheme to secure online social networking content with multiple owners" Proc SPIIE11137, Applications of Digital Image Processing XLII, San Diego, California, United States. pp. 111371M1- 111371M9, 2019, doi: 10.1117/12.252987.

vi. **Sonal Kukreja**, Singara Singh Kasana, Geeta Kasana, “Random Grid based Extended Visual Secret Sharing Scheme for Image Authentication", 8th International Conference on Cloud Computing, Data Science and Engineering, Confluence, pp. 870-875, 2018, doi: 10.1109/CONFLUENCE.2018.8442463.

CHAPTER 1

Introduction

Protection of the sensitive data being transmitted on the network is a significant concern with the rapid developments in information and multimedia technology. The transmitted digital data may be in any form such as text, images, audio and video. The channels used in these communication are not perfectly secure, due to which these data need be protected from unauthorised users. A lot of schemes have been introduced over the last few years to protect digital data in different applications. Secure digital imaging is a critical research field that involves numerous forms of data-securing schemes: cryptography, steganography, and watermarking. In cryptography, the data is scrambled into an unreadable form using a key. The same or different key is used at the receiver's side to unscramble. In watermarking and steganography, the secret data bits are embedded in the cover media without any perceptual distortion or scrambling, thereby creating marked media. In steganography, the purpose of hiding data is to protect the secret data while in watermaking the aim is to protect the cover media. This Chapter starts with an explanation of cryptography, Visual Cryptography (VC) and watermarking. Our research work focuses on watermarking systems based on *VC* that are used to secure the copyright and authenticate digital images. Here we present an overview of the base model for these schemes.

1.1 Cryptography

Cryptography is a technique to encrypt data and communication by encoding it using a set of mathematical rules, so that intended users can decrypt and access it. The basic block diagram of cryptography is shown in Figure 1.1. The most commonly used terms used in any cryptography scheme are as follows:

i. Plain Text: Data requiring protection is known as plain text.

ii. Cipher Text: Cipher text is regarded as encrypted data which can only be accessed by intended users.

iii. Encryption: The method of transforming plain text to cipher text using a set of rules and key is called encryption.

iv. Decryption: The method of transforming cipher text to plain text using a set of rules and the key is called decryption.

v. Cryptanalysis: An effort to translate cipher text to plain text without the knowledge of the encryption algorithm and/or key is referred to as cryptanalysis.

vi. Key: Key is a random binary bit sequence used to encrypt and decrypt data.

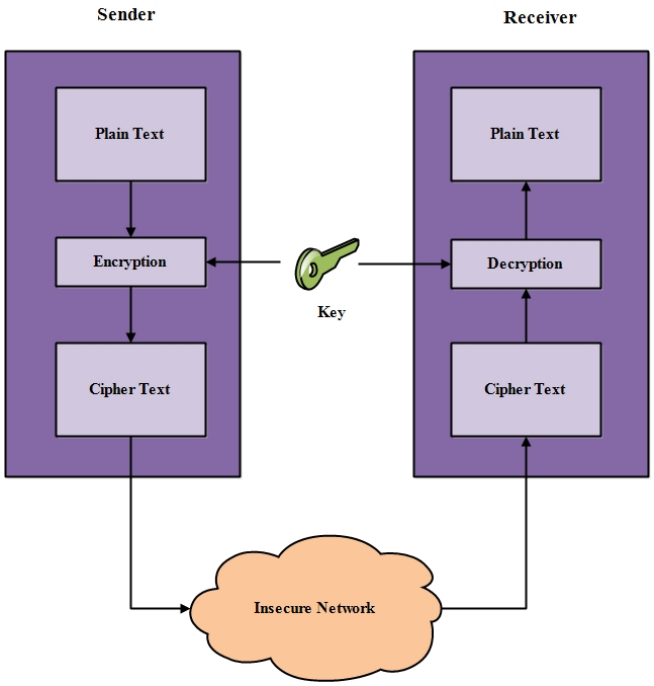


Figure 1.1: Block Diagram for Cryptography

Different traditional cryptography (Gangopadhyay et al. (2017)) encryption methods have been used in the past eras to protect the information. Visual information protection (e.g., confidential image, handwritten notes, digital data, and printed text, etc.) is a challenging security issue. It has been a field of prime concern since the world's digitalisation started two decades ago. Secret Image Sharing is an important field of study, incorporating approaches and techniques from both cryptography and image processing. It helps securing visual information.

1.2 Visual Cryptography

VC is a special cryptography scheme proposed by Naor and Shamir (1994) for digital images that do not need any complex decryption algorithm as it can be done by simply superimposition of the shares. The concept of *VC* was based on secret sharing described by Shamir (1979). This section provides a description of the secret sharing and *VC*.

1.2.1 Secret Sharing

Secret sharing proposed by Shamir (1979), is a special cryptography scheme where secret is divided into parts and distributed among participants. To reconstruct the secret a certain number of participants are required. The part of the secret with every participant is called a share. The individual shares will not disclose any detail about the confidential information until they are superimposed on each other. This scheme can be described as:

Let *IN* be the information to be exchanged between n participants. Thus the threshold scheme *(k, n)* divides this *IN* into n shares IN_1, IN_2, IN_3, ..., IN_n based on following conditions:

- *IN* can be retrieved completely by combining k or more shares.
- Any information about *IN* cannot be obtained from less than k shares.

For example, if there is a bank vault whose key has been shared with seven users, and it was decided that any *4-out-of-7* user can access that vault for security purposes and no less than seven attendees can access it. This is known as the threshold scheme *4-out-of-7*. The representation is shown in Figures 1.2 and 1.3, where the secret data is distributed among seven participants, and atleast four participants are required to decrypt it.

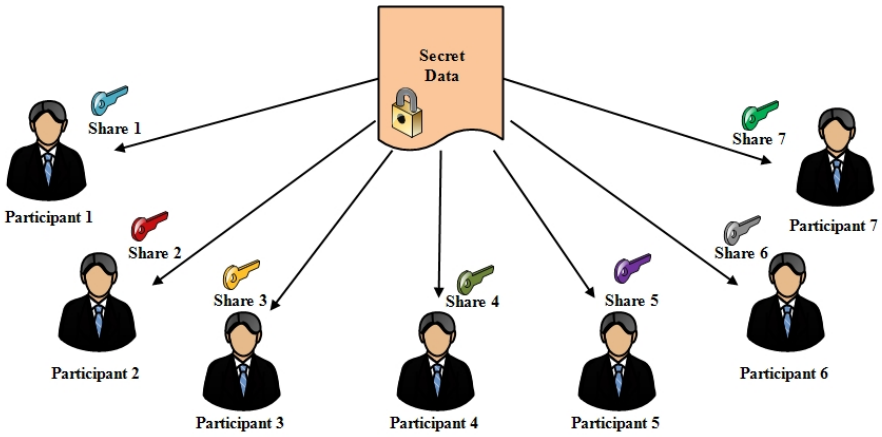


Figure 1.2: Shares of Secret Data shared among 7 Participants

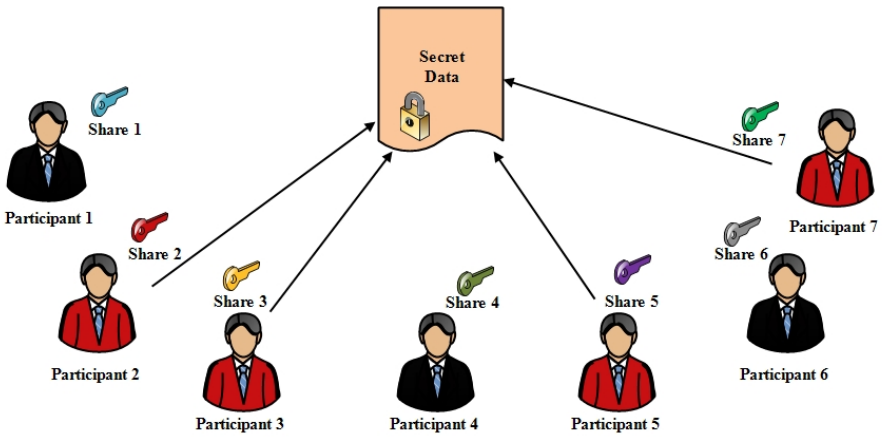


Figure 1.3: Reconstruction of Secret Data when k=4, n=7

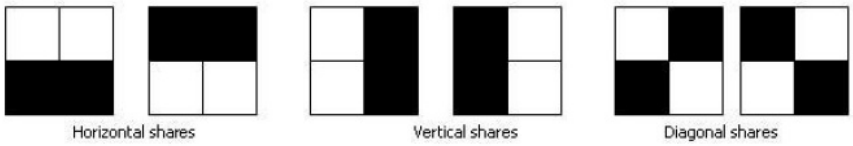


Figure 1.4: Representation of shares corresponding to black pixel of the original image

1.2.2 Overview of Visual Cryptography

Based on secret sharing schemes, Naor and Shamir (1994) proposed a scheme for sharing a secret image between n participants in such a way that each participant would obtain a share. This is a variant of the standard encryption schemes. Decryption does not need any complex calculations or cryptographic algorithms, but the data is retrieved back simply when atleast k shares are superimposed using binary logical operations. This is referred as k-out-of-n VC scheme . VC has many applications(Liu and Yan (2014)) data hidng, copyright protection, visual authentication, identification, *etc.*

Naor and Shamir (1994) scheme was initially implemented for binary images. The key limitation to this scheme is that the contrast between the received image and the initial image is reduced. Contrast is a key parameter in *VC*, as it defines how clearly the secret image will be visible to human eyes. Later, various schemes for grayscale and color images were also proposed, that enhanced the contrast Blundo et al. (2003).

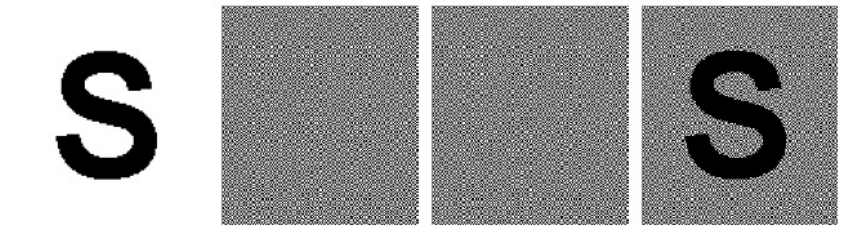
The collections Z_0 and Z_1 for *(*2,2)*-VC* have been defined as follows:

Z_0 = all matrices obtained by permuting the columns of $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$

Z_1 = all matrices obtained by permuting the columns of $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$

Z_0 and Z_1 of size $n \times m$ represent collections for white and black image pixels, respectively. n and m represents number of participants and number of sub-pixels in the share block, respectively. To create the shares, for every white pixel of the secret image, any two rows are chosen from Z_0, which have the same patterns of four subpixels. While, for every black pixel, any two rows are chosen from Z_1 that represent complimentary patters of four subpixels. These patterns has been shown in Figure 1.4.

Shares should be precisely aligned and then superimposed. Superimposition is equivalent to the binary logical *OR* operation applied among the corresponding share pixels. Individual shares



(a) Secret Image (108×121) (b) Share 1, S_1 (216×242) (c) Share 2, S_2 (216×242) (d) Restored image, $S_1 + S_2$ (216×242)

Figure 1.5: Implementation of *(2,2)-VCS*

don't provide any information about the pixels, so it's impossible to decrypt the shares even by using large computations. If the shares are superimposed, the outcome of the superimposition of the identical subpixel patterns of the two shares will be a white pixel, but if two different subpixel patterns overlap, the outcome will be a black pixel. Thus, the secret image will be retrieved from the two shares. Figure 1.5 displays the implementation of (2,2)-VC. Two shares (Figure 1.5-(b) and (c)) have been generated for a secret image (Figure 1.5-(a)), and when those shares are superimposed, the secret image is recovered back. One can observe there is a loss of contrast (Figure 1.5-(d)). Also, this scheme experiences pixel expansion, since there is a corresponding block of four subpixels in the share per each pixel in the secret image.

1.2.3 Variations in Visual Cryptography

The traditional *VC* schemes were further extended(Weir and Yan (2010); Weir (2011)) in the past few decades and can be summarized as follows:

Size Invariant Visual Cryptography Schemes

Traditional VC schemes show pixel expansion, which results in higher share storage and transmitting costs. A lot of research has therefore been conducted on how to improve this. The size invariant scheme in *VC* was first proposed by Ito et al. (1999) where pixel expansion was eliminated. The author used the standard *(k,n)* scheme with m=1, where m refers to subpixel count in the shared image block, should be one in this case.

A boolean n-vector $X = [x_1, x_2, ..., x_n]^T$, was used to define the structure of the scheme, where x_i is the color of the pixel in the i^{th} share.

$x_i = 1$ represents a black pixel,

$x_i = 0$ represents a white pixel.

The decryption process is similar to the traditional *VC* schemes. Similar to the standard *VC*, this scheme can also be expressed by $n \times m$ matrices described as:

$$C_0 = \text{ set of matrices resulted by the permutation of columns of } \begin{bmatrix} 1 & 0 & 0 & . & . & . & 0 \\ 1 & 0 & 0 & . & . & . & 0 \\ . & . & . & . & . & . & . \\ 1 & 0 & 0 & . & . & . & 0 \end{bmatrix}$$

$$C_1 = \text{ set of matrices resulted by the permutation of columns of } \begin{bmatrix} 1 & 0 & 0 & . & . & . & 0 \\ 0 & 1 & 0 & . & . & . & 0 \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & . & 1 \end{bmatrix}$$

In this scheme m is always one as there is no pixel expansion and n depends on the scheme being used. For example, suppose 3 shares have to be generated for a secret image. Using the matrices set C_0 and C_1, $n \times m$ matrices S_0 and S_1 are chosen at random from C_0 and C_1 :

$$S_0 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

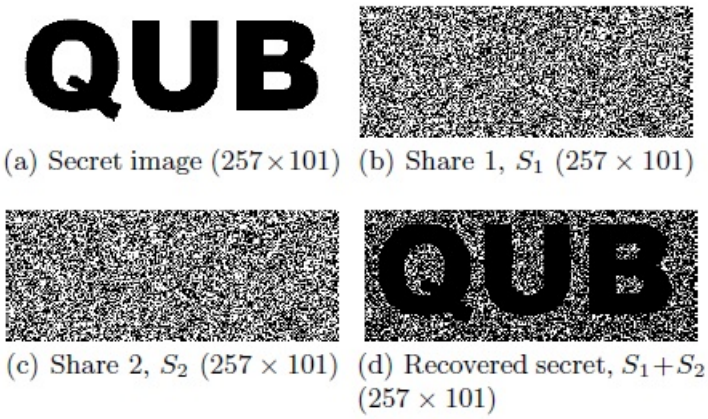
$$S_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

For every white and black pixel in the secret image, any one of the columns of S_0 and S_1 respectively, is chosen for the shares. The values in the selected column vector $X = [x_1, x_2, ..., x_n]^T$ would represent the color of the pixel in the respective shares, *i.e.* x_i refers to the pixel color in the i^{th} share. This scheme was futher improved in Yang and Chen (2005a, 2006).

Extended Visual Cryptography Schemes

The concept of VC was further proceeded by the development of some meaningful shares, as the noisy shares had the disadvantage of being suspected of carrying some confidential information. When the shares are superimposed at receiver's side, the meaningful information vanishes and the secret contained inside the shares is retrieved.

Ateniese et al. (1996) proposed the first extended variation of *VC* with regard to its general access structure and enhanced functionality. They introduced noiseless meaningful shares instead of the



(a) Secret image (257×101) (b) Share 1, S_1 (257 × 101)

(c) Share 2, S_2 (257 × 101) (d) Recovered secret, S_1+S_2 (257 × 101)

Figure 1.6: Implementation of SIVCS

random noise shares in Naor and Shamir (1994). In Extended Visual Cryptography Scheme (EVCS), the general structure is of the form $(\tau_{qual}, \tau_{forb})$. This structure represents a set of n shares. The shares belonging to the sets of the qualified set ($x \epsilon \tau_{qual}$) have the ability to recover the secret image by superimposing each other, and any share belonging to the set of forbidden shares ($x \epsilon \tau_{forb}$) can not reveal any knowledge about the secret image.

The *EVCS* requires the assurance of following conditions:

i. The secret image should be revealed only when the shares of the qualified set access structure are superimposed. This state is classified as the *contrast state* (Pandey and Ghanekar (2015); Ghanekar et al. (2009); Anwar et al. (2017); Anwar and Khosla (2017)).

ii. The individual shares should not have the ability to reveal the secret. This is classified as *security condition.* (Asuquo et al. (2018); Cruickshank (1996))

iii. The image contained inside the shares should not be distorted, *i.e.* the superimposition of the meaningful shares should be able to display the original image to the user.

The Figure 1.7 is an example of *(2,2)*-EVCS. The figure indicates that two meaningful shares have been created from the secret image. The superimposition of these shares retrieve secret image.

In the case of *EVCS*, the quality of shares has been improved in Yang and Chen (2005b) , by using gray subpixels instead of black and white subpixels by the process of halftoning. Many other improvements have been done in this area to improve the quality of shares, reduce the pixel expansion and apply it to color images as well.

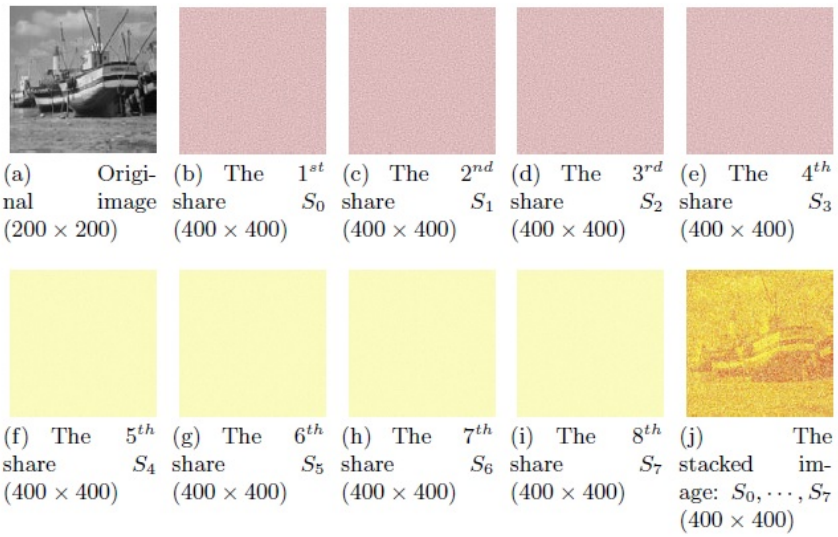
Figure 1.7: An examaple of (2,2)-*EVCS*

Visual Cryptography Schemes for Halftone Error Diffusion

As the traditional Naor and Shamir (1994) scheme was only feasible for binary images, the idea of halftoning was implemented to extend it to grayscale and color images. Halftoning is a continuous tone modelling scheme with the help of dots that differ in size or space () Campbell (2000)). In the case of halftoning, the secret images are transformed to halftone images to which VC schemes are applied. Blue noise halftoning is used to produce halftone shares during the construction process. The secret image retrieved preserves an uniform contrast. Half-tone shares are capable of providing substantial information to users, and their visual quality is much better than traditional schemes. Thus, the adversaries can not suspect that some cryptographic information has been concealed within the shares.

Visual Cryptography Schemes for Color Images

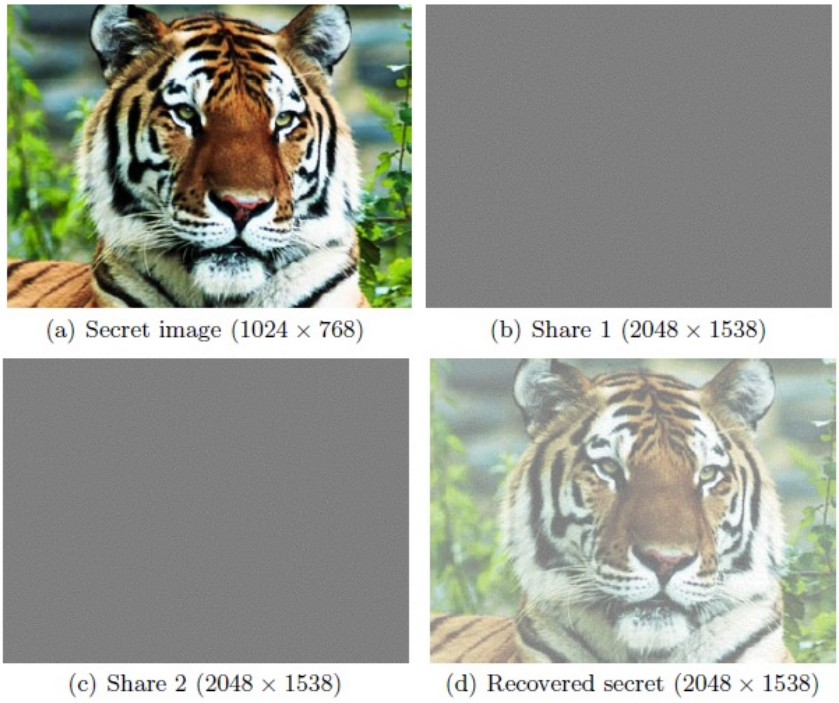
One of the most important area of research in VC is to apply it on natural color images. Many of the schemes proposed involved the concept of halftoning, *i.e.* first converting the color image into a binary image and then using the traditional VC schemes. Naor and Pinkas (1997) extended their first approach bringing significant improvements. One transparent color and two opaque colors were used in this scheme. Instead of a single transparency, every participant now had c sheets, and every sheet had red, yellow and transparent pixels. And the secret was recovered by superimposing the respective sheets of the shares. The construction of shares was carried out in two ways: monochromatic construction and bichromatic construction. This scheme has been shown in the Figure 1.8 and Figure 1.9 for *(2,2)-VC* scheme for color images. It should be observed that before processing the original grayscale image, it first undergoes pre-halftoning.



(a) Original image (200×200) (b) The 1^{st} share S_0 (400×400) (c) The 2^{nd} share S_1 (400×400) (d) The 3^{rd} share S_2 (400×400) (e) The 4^{th} share S_3 (400×400)

(f) The 5^{th} share S_4 (400×400) (g) The 6^{th} share S_5 (400×400) (h) The 7^{th} share S_6 (400×400) (i) The 8^{th} share S_7 (400×400) (j) The stacked image: $S_0, \cdots, S_7$ (400×400)

Figure 1.8: Implementation of monochromatic construction for (2,2)-VCS using a cover base



(a) Secret image (1024×768) (b) Share 1 (2048×1538)

(c) Share 2 (2048×1538) (d) Recovered secret (2048×1538)

Figure 1.9: Example of (2,2)-VCS for color images

Visual Cryptography Schemes for Multiple Secrets

The schemes which have been discussed earlier were responsible for sharing just a single secret. The extension to it was hiding more than one secret within the two shares, hence increasing the secret sharing capacity. Many schemes were proposed to to increase the amount of the embedded information.

In multiple secret sharing schemes(Weir and Yan (2010)), two secret images can be hidden inside two shares. When both the shares were superimposed, the first secret image was retrieved and the second secret image was retrieved when the first share was rotated by 90°in anticlockwise direction and then superimposed on the second share. The main drawback of this scheme was that it could share atmost two secrets and also there was limitation on angles *i.e.* the value of degree of rotation could be 90°, 180°or 270°.

1.3 Watermarking

Watermarking is a technique of hiding data in the host carrier media, such that the hidden data does not need to be related to the host media. Watermarks are used to verify the authenticity or integrity of the host or to prove the identity of its own owners.

Digital watermarking refers to the process of watermarking the digital images. Watermarked images should be robust. *i.e.* even if the marked images experience multiple intentional or unintentional image processing attacks, the watermark should be extracted without any distortion in the host image. Also, only authorized receivers should have the ability to extract the watermark embedded in the marked image, without any ambiguity. Hence, watermarking is typically used to detect copyright infringements, to settle conflicts between the malignant receiver and the owner. For example, if an owner makes his images available online for free, he should embed a watermark in the images to avoid the misuse and false copyright issues. Thus, the images can be downloaded by anyone and if some dispute arises, it can be resolved by extracting the watermark.

Watermarking may be used in various roles such as broadcast monitoring (Salameh et al. (2017, 2018)), owner identification, copyright protection, authentication (Lin et al. (2006, 2011) copy control, device control (Muhammad et al. (2017); Braik et al. (2007)), legacy enhancement, etc.

Watermarking systems are applied in two phases:

i. Embedding: Here, the watermark is embedded in the original host image using numerous embedding schemes available.

ii. Extraction: Here, the watermark is extracted from the marked image using the inverse procedure of the embedding scheme.

All watermarking schemes (Singh and Singh (2017a,b); Singh et al. (2018)) have different properties based on the application scenarios under which the watermarking is used. These properties are discussed as follows:

i. **Embedding Effectiveness:** It is the probability that the image will be marked successfully during the embedding process.

ii. **Imperceptibility:** This property refers to the distortion generated by the watermark embedding in the image, which should be minimal.

iii. **Blind or Knowledgeable Detection:** In some cases, an original image or other related information is also needed for the recovery of the watermark during the extraction process. This is regarded as Informed detection, shown in Figure 1.10. While scenarios where no information on the original data is provided during the extraction process, are known as Blind detection, shown in Figure 1.11.

iv. **Robustness:** This property refers to the ability of the scheme to extract watermark image in an identifiable format from the marked images that have been targeted by numerous attacks, such as compression, cropping, graphical distortion, scaling, noise, rotation, etc.

v. **Security:** This property guarantees that only authenticated users have the right to extract watermarks from a marked image. (Truong et al. (2019); Al-Dahhan et al. (2019))

vi. **Unambiguity:** The watermark should be removed and tested for ownership of the host image without any uncertainty.

1.3.1 Classification of Watermarks

The watermarks can be classified into three categories on the basis of the applications where they are used:

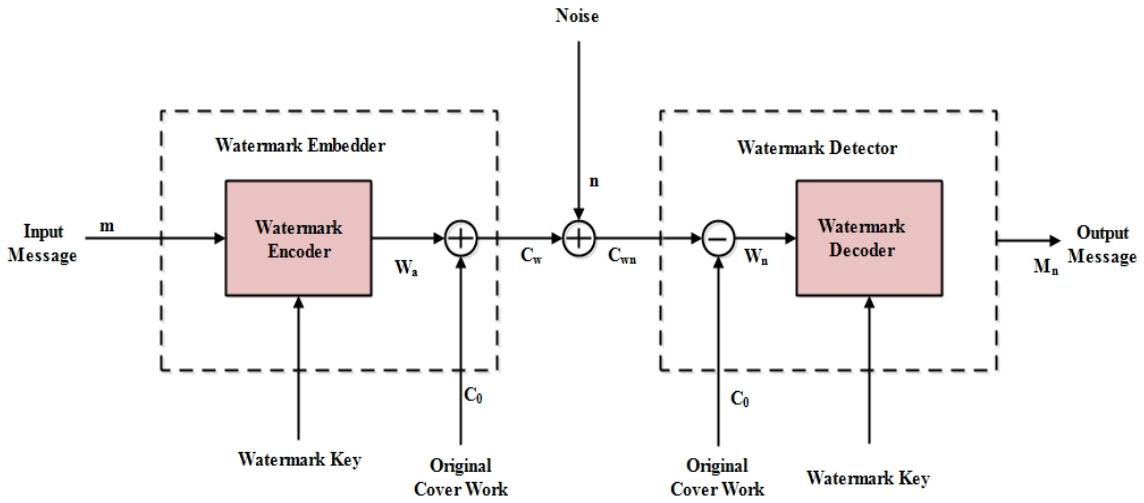


Figure 1.10: Watermarking System using Informed Detector

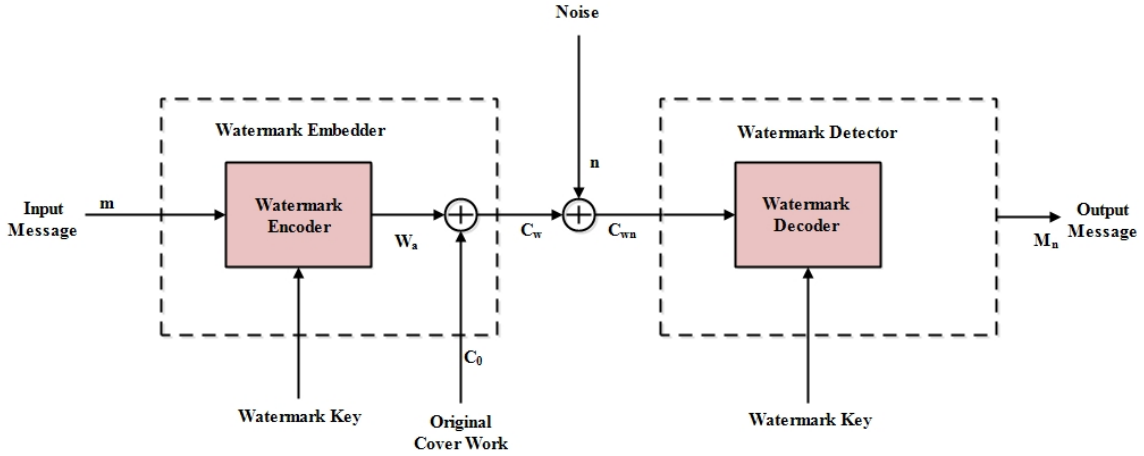


Figure 1.11: Watermarking System using Blind Detector

i. **Robust Watermarks:** Some watermarking schemes require watermarks that can withstand image processing attacks, *i.e.* even when an attempt is made to modify the image, the watermark should not be affected. Such schemes are used to protect the copyright of digital images, where even if the images are attacked, the scheme should have ability to prove the copyright. (Shie and Lin (2008))

ii. **Fragile Watermarks:** Some applications like image authentication require fragile watermarks, *i.e.* if the image is tampered, the embedded watermark should also be tampered that help in detecting if the images are tampered, localizing the tampered areas and also recovering it. (Lin and Yang (2011); Lee and Lin (2008))

iii. **Semi-Fragile Watermarks:** In case of semi fragile watermarking schemes, the image modifications occur unintentionally, such as bit errors during transmission, signal processing operations like contrast enhancement, compression, *etc.* Semi fragile watermarks are more robust than fragile watermarks but lesser than the robust watermarks.

1.4 VC Based Watermarking Schemes

In the traditional watermarking schemes, the watermark is embedded into the host image which modifies the image and affects its visual quality. In last two decades *VC* based watermarking schemes have gained a lot of attention. In these schemes, host image can be protected without embedding watermark into it. A separate share is created using some significant features of the host image, which is referred as Master Share (MS). Another share is created using *MS* and an external watermark, which is known as Ownership Share (OS). This share is stored with the *TA*. At the receiver side, the watermark is retrieved by superimposing the shares without any complex computations.

In this thesis, two prime applications of watermarking *i.e.* copyright protection and authentication have been worked upon.

1.4.1 Copyright Protection Schemes using VC

The *VC* based copyright protection schemes are carried out in two ways. In the first approach, one or more shares are generated using *VC* that are then embedded into the host image to create watermarked image. This scenario, does not utilize the characteristics of *VC* judiciously to extract

the watermark by superimposition, as these type of schemes employ an extra process to hide the data that increases the complexity of the schemes at the receiver's side during extraction.

In the second approach, *MS* results from the host image. This along with the watermark generates *OS* that is stored with the *TA*. When the need arises to prove the copyright, *MS* is created again from the claimed host image using the same approach as before. This *MS* is then superimposed with the stored *OS* to retrieve the watermark. The resemblance of the retrieved watermark with the original watermark helps in proving the copyright of the image.

1.4.2 Authentication Schemes using VC

Similar to copyright protection schemes, the *VC* based authentication schemes are also carried out in two ways. In the first approach, the shares constructed from the host image along with the authentication bits are embedded into the cover image to create meaningful shares which are transferred through the communication channels. At the receiver's side, the authentication bits are calculated from the received host image and compared with the extracted authentication bits from the meaningful shares. Their similarity verifies the authenticity of the host images.

In the second approach, an additional authentication share is created to authenticate the image instead of embedding the shares inside the cover images. These schemes create meaningful shares from the watermark and cover images using the properties of *VC*. This helps in reducing the computational complexity at the receiver's side, as here the authentication data can be retrieved just by superimposing the shares.

1.5 Motivation of the Proposed Work

- Existing copyright protection and authentication schemes based on VC and Watermarking generate only meaningless random shares for the watermark, which lead to lesser security, as the random looking shares create an impression that some confidential information is being stored or transferred.

- The existing copyright protection schemes based on *VC* and watermarking use *(2,2)-VC* which leads to some gaps in security and robustness of the scheme, as in that case only one participant is involved, and in the case of failure, the watermark cannot be retrieved back if the share

with the participant is lost or damaged.

- The existing copyright protection schemes have low *PSNR* for the attacked host images and low *NC* of the extracted watermark from the attacked images.
- Copyright Protection schemes based on *VC* and watermarking, using multiple watermarks to protect the cover image for multiple hosts have not been studied much.
- Color images have not been much studied for the copyright protection and authentication using *VC* and Watermarking, as most of them work on binary and grayscale images.

1.6 Thesis Contribution

The thesis makes the following contribution:

i In all the proposed copyright protection and authentication schemes, meaningful ownership shares have been constructed that provides security to the shares being stored or transmitted.

ii Pixel expansion has been removed in the image authentication schemes by using *CA*. The self construction ability of *CA* also helps in eliminating the use of codebook. This saved transmission and storage cost.

iii In all the proposed authentication schemes, meaningful shares are created utilizing the *VC* characteristics and without any additional data hiding technique. This saves the computational cost, as the watermark is retrieved just by superimposition.

iv To deal with the cases of false positives, difference color channels *i.e.* C_b and C_r channels of the image have been used to create an additional watermark. This self constructed watermark contains image information, hence only the authorized owners of the image can claim the copyright.

v A copyright protection scheme for numerous images with numerous owners is proposed by using *SURF* and *LBP*. The robustness against rotation attack has been improved by using LBP. The frequency of keypoints used for SURF permits watermark size flexibility.

1.7 Methodology

- After doing a review of the existing copyright protection and authentication schemes based on VC, four schemes are proposed to address the mentioned gaps in the existing schemes. In all of the proposed techniques, meaningful and noiseless shares are created, which are then superimposed on each other to verify the copyright of the host image.

- Robustness of the proposed copyright protection schemes is tested and proved against various image processing attacks like blurring, sharpening, rotation, scaling, JPEG compression, noise addition, cropping, etc.

- Authentication schemes are proposed in which the image is authenticated by generating meaningful authenticated shares with size equal to the original image.

- As mentioned in the Literature survey and the gaps, the existing copyright protection schemes based on VC and watermarking use (2,2)- VC, which involves only one participant. Thus generalized (k,n)- VC schemes are proposed to ensure robustness of the entire copyright protection scheme.

- The proposed copyright protection scheme(s) can be applied to multiple hosts, thus protecting multiple images.

- Proposed scheme(s) are extended to color images by exploiting the correlation between its different color channels.

- All of the simulations' images are from the *USC-SIPI* Image Database (Weber (1997)), database of the Computer Vision Group at the University of Granada (Aranda et al. (2000)) and *CSIQ* database (Larson and Chandler (2010)).

- To evaluate the performance of the Copyright Protection and authentication schemes, these parameters might be considered:

    i. **Peak Signal to Noise Ratio**: Peak Signal to Noise Ratio (PSNR) is calculated between two images and is the metric that has widely been used in literature for establishing image

visual quality. It is a function of Mean Square Error (MSE) and is defined as,

$$PSNR = 10 \times log_{10} \frac{(2^{bd} - 1)^2}{MSE} \tag{1.1}$$

where bd is the bit depth of the image and MSE is defined as,

$$MSE = \sum_{x=1}^{M} \sum_{y=1}^{N} \frac{\delta(x,y)^2}{M \times N} \tag{1.2}$$

where $\delta(x,y)$ is defined as

$$\delta(x,y) = I(x,y) - I'(x,y) \tag{1.3}$$

where $I(x,y)$ and $I'(x,y)$ are the pixels of two images being compared, M and N is the height and width of image respectively.

ii. **Normalized Correlation**: The Normalized Correlation (NC) is used to measure the correlation between two images and is defined as:

$$NC = \frac{\sum_{m=1}^{M} \sum_{n=1}^{N} \overline{(I(m,n) \oplus I'(m,n))}}{M \times N} \quad \ldots (1.4)$$

where $I(m,n)$ and $I'(m,n)$ represent the two images being compared, $\oplus$ denotes the Exclusive-OR (XOR) operation and $M \times N$ is the size of image.

iii. **Structural Similarity Index**: Structural Similarity Index (SSIM) calculates similarity for various image windows to determine how similar two images are. The measure of similarity between two windows of the same size is:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad \ldots (1.5)$$

where x and y are the two different windows, $\mu_x \ and \ \mu_y$ are the average values of x and y , $\sigma_x^2 \ and \ \sigma_y^2$ are the variance of x and y, σ_{xy} is the covariance of x and y, $c_1 \ and \ c_2$ are two variables to keep the division stable where $c_1 = (k_1 L)^2)$, $c_2 = (k_1 L)^2)$, L is the dynamic range of the pixels, $k_1 = 0.01$ and $k_2 = 0.03$ taken as default.

iv. **Bit Error Rate**: Bit Error Rate (BER) is defined as:

$$BER = \frac{I}{M \times N} \quad \ldots(1.6)$$

where $M \times N$ is the size of the watermark image, and I represents the number of received watermark bits that have been modified due to noise. The range of BER is [0, 1].

v. **Tamper Assessment Function**: Tamper Assessment Function (TAF) is defined as follows:

$$TAF = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} I(x,y).I'(x,y) \quad \ldots(1.7)$$

where I and I' represent the original and extracted watermark respectively, $A.B$ represents AND operation between A and B, and $M \times N$ is the size of watermark.

vi. **Normalized Hamming Similarity**: This parameter is used to determine how similar two images are. Normalized Hamming Similarity (NHS) is defined as:

$$NHS = \frac{HD(I,I')}{N \times N} \quad \ldots(1.8)$$

where HD is the hamming distance between two binary images, I and I' are two images of size $M \times N$.

To test the effectiveness of the proposed scheme's tamper detection ability, some additional parameters are used. These parameters are described in Table 1.1. Two cases have been considered for this evaluation:

(i) Case A: In this case, the efficiency of tamper detection is measured in terms of the number of pixels in the image.

(ii) Case B: In this case, the efficiency of tamper detection is measured in terms of the number of blocks in the image.

Table 1.1: Parameters used for Statistical Analysis of Tamper Detection

Parameter	Description
T_{pixels}	Total number of pixels in I
X_{pixels}	Total number of tampered pixels in I

Table 1.1 continued from previous page

T_{blocks}	Total number of blocks in I
X_{blocks}	Total number of tampered blocks in I
True Positive (TP)	A true positive is an outcome where the model correctly predicts the positive class *i.e.* number of tampered pixels or blocks that are accurately identified as tampered.
True Negative (TN)	A true negative is an outcome where the model correctly predicts the negative class. *i.e.* number of untampered pixels or blocks that are accurately identified as untampered.
False Positive (FP)	A false positive is an outcome where the model incorrectly predicts the positive class. *i.e.* Number of pixels or blocks that are tampered but falsely identified as untampered
False Negative (FN)	A false negative is an outcome where the model incorrectly predicts the negative class.*i.e.* Number of pixels or blocks that are untampered but falsely identified as tampered
False Positive Rate (FPR)	$\frac{FP}{FP+TN}$
True Positive Rate (TPR)	$\frac{TP}{TP+FN}$
Accuracy (%)	$\frac{(TP+TN)}{(Total\ number\ of\ pixels\ or\ blocks)}$

The images can be unethically modified by the unauthorized users during the transmission. According to Voloshynovskiy et al. (2001), different image processing attacks are divided into various categories like image enhancement, cropping, rotating and compression. While, Kutter and Petitcolas (1999) divided these attacks into different categories based on their properties which are described as follows:

i. **Geometric Transformation Attacks**: These attacks include rotation, resizing and cropping that modify the image's geometry when applied.

   (a) **Rotation**: In this attack, a set of pixels is rotated by an angle $\theta 8$ about the origin, either counterclockwise or clockwise. This can be expressed as $x' = x \times cos\theta + y \times sin\theta$ and $y' = -x \times sin\theta + y \times cos\theta$, where θ specifies the rotation angle. For example, Rot(10) rotates a set of pixels clockwise by an angle θ=10 about the origin.

(b) **Cropping Attack**: To focus on a specific part of the image, a certain part is cropped and rest of the image is neglected. For example, in Crop(50) the image is cropped to 50% of the original size.

(c) **Resizing**: Images can be resized intentionally or unintentionally in uniform or non-uniform manner.

ii. **Noise Addition Attacks**: In these attacks, additive and uncorrelated multiplicative noise is added to the images.

(a) **Gaussian noise**: Gaussian noise manipulates the variations of the intensity drawn from a Gaussian normal distribution. The noise value is added to the pixels of the input image. Its amount can be adjusted by a single parameter ranging from 0 to 100 where 0 means no noise and 100 means completely random image. For example, Noise(20) adds the noise value=20 to the pixels of the host image.

(b) **Poisson noise**: Here, instead of adding any artificial noise to the image, the noise is added from the image data itself.

(c) **Salt and Pepper Noise**: During the data transmission, some pixels get modified and is set to zero or maximum value, that gives a salt and pepper appearance to the image.

(d) **Speckle Noise**: Here, the speckle is a multiplicative noise that spreads inherently as granular noise. The pixels are modified in such a way that the variance of modified pixels equals the variance of the pixels surrounding it.

(e) **Sobel Attack**: This attack detects the edges and returns the image with the detected edges.

iii. **Enhancement Technique Attack**: The objective of common enhancement techniques like median filter, blurring and sharpening is to enhance the quality of the images they are applied on.

(a) **Median Filtering**: In this attack, $M \times N$ pixels are processed, such that each pixel is replaced with the median intensity value of its region. For example, Median(5) will operate over a block of 5×5 pixels such that each pixel's value is replaced with the median intensity of its region.

(b) **Sharpening**: This attack detects high frequency noise introduced by unauthorized users. Sharpening enhances gray-scale and color images.

(c) **Blurring**: This attack works opposite to the sharpening attack as it attenuates the high spatial frequencies. In contrast to sharpening, blurring attack spreads out the information from every pixel to the pixels in surrounding region.

iv. **JPEG Compression**: In JPEG compression, the pixels are processed and compressed in lossy manner with quality factors in range 0-100. These pixels need less memory to be represented. After the images are JPEG compressed, there is a loss in sharpness, edge clarity, color details as quality factor tends to 0. For example, JPEG(8) is a lossy representation of the processed pixels with quality factor=8.

1.8 Thesis Organization

The thesis is organized as follows: Chapter 1 presents the general introduction to *VC* and watermarking. It also discusses how the characteristics of *VC* can be utilized to protect the images without embedding the watermark. Chapter 2 provides a thorough literature review of the existing copyright protection and authentication schemes. From this review, the gaps in these schemes have been identified. These gaps are used to formulate objectives. Chapter 3 presents a proposed authentication scheme based on Wavelet Packet Decomposition (WPD) and Cellular Automata (CA) where no embedding into the cover images is performed and meaningful authentication shares are created. Chapter 4 presents a robust copyright protection scheme based on Discrete Curvelet Transform (DCuT), k-means Clustering, Baker Map and *EVCS* for color images. Chapter 5 presents an enhanced copyright protection scheme using DCuT, k-means Clustering, Henon Map and *EVCS*, that handles false positive cases efficiently. Chapter 6 presents an *EVCS* based copyright protection scheme for multiple images and owners using *SURF* and *LBP*. The proposed techniques have been concluded in Chapter 7. Also the possible future scope have been discussed.

CHAPTER 2

Literature Survey

Existing *VC* based watermarking schemes for digital images are reviewed in this Chapter and several gaps in these schemes have been identified. On the basis of these gaps, the objectives and methodology of the proposed work have been identified, leading to the formulation and solution of the problems addressed in the following Chapter.

2.1 Copyright Protection Schemes using VC

VC based watermarking schemes have gained a lot of popularity as they have the potential to secure the digital images without embedding watermark. Indeed, at the receiver's side, *VC* allows reconstruction of the watermark by just superimposing the shares stored with the owners or *TA*. These schemes take advantage of *VC*'s properties in two ways: Using *VC*, one or more shares are generated from the watermarks in the first option. These generated shares are embedded in the host image, resulting in a watermarked image that is sent over transmission channels. In the second method, a share called *MS* is formed from the host image, which is then joined with the watermark to create another share called OS. The *TA* keeps track of this share. When the need arises to prove the copyright, The claimed host image is used to rebuild *MS*. This *MS* is then superimposed with the stored

OS to recover the watermark. The image's copyright can be established by comparing the retrieved watermark to the original watermark.

The *VC*-based watermarking techniques can be divided into two types based on the master share construction: (1) spatial domain features based and (2) frequency domain features based.

2.1.1 Spatial Domain Features Based

This section discussed the schemes that use spatial domain features to create the shares. In these schemes, *MS* is generated using the spatial relationship among image pixels.

Embedding Based Scheme

Hou and Chen (2000) proposed the first digital watermarking scheme based on *(2,2)-VC*. Using the Naor and Shamir (1994) method, two noisy random seeming shares are formed from the watermark, one of which is incorporated in the host image and the other of which is kept as a secret key share with *TA*. At the receiver's side, this secret share is then superimposed on the extracted share to obtain the watermark. The main advantage of employing *VC* for watermarking is that the watermark may be extracted without the use of complex computational or computerised extraction procedures. The watermark may be removed by simply superimposing it on top of the share mage, which is immediately visible to human eyes. The scheme shows to be robust to a range of attacks. This scheme is described in Figures 2.1 and 2.2.

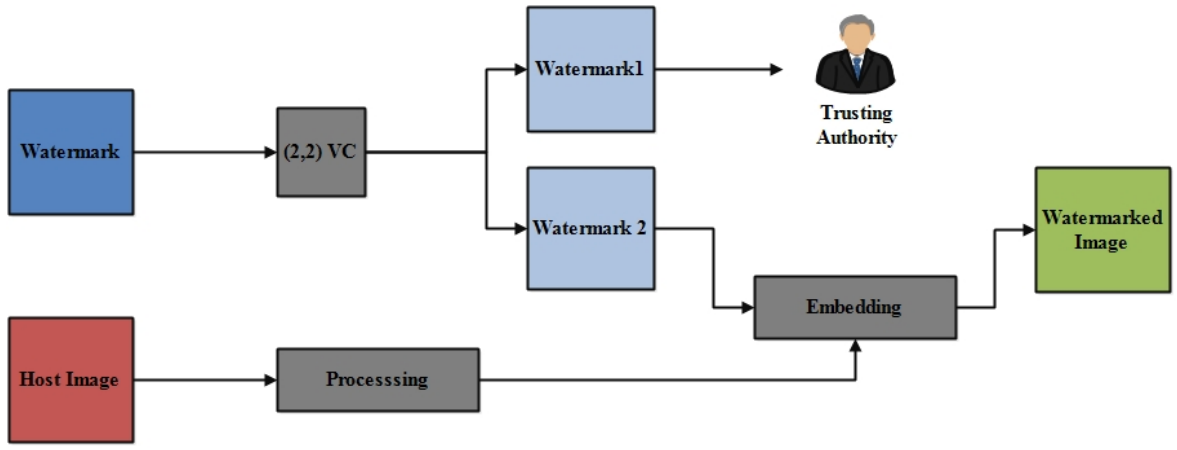


Figure 2.1: Spatial Domain: Share Creation and Embedding

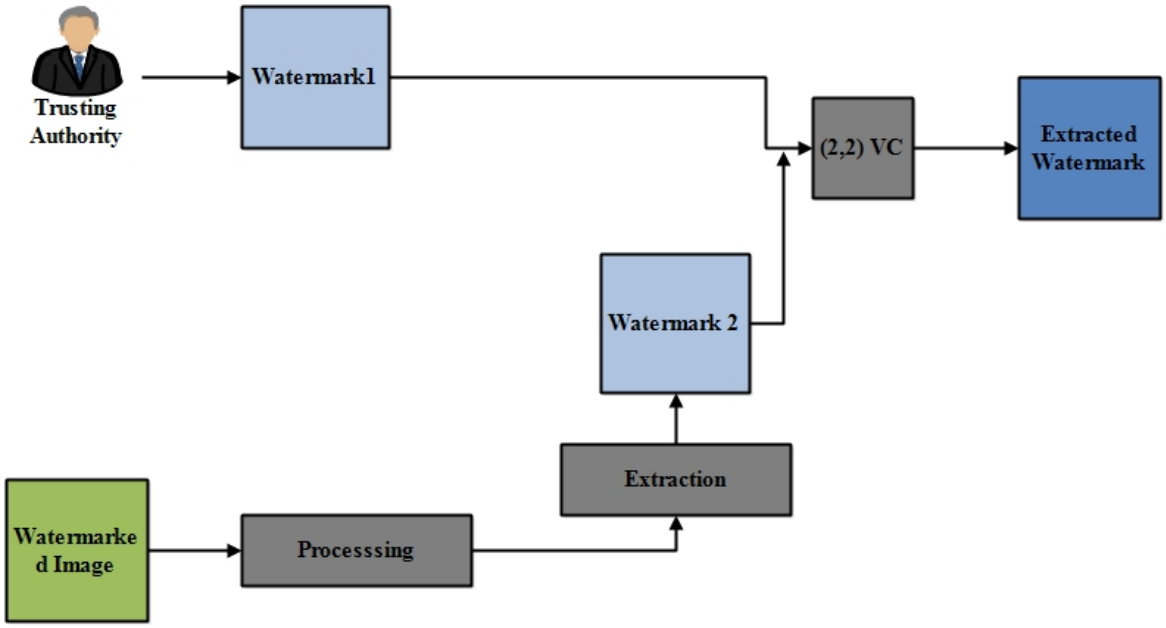


Figure 2.2: Spatial Domain: Share Extraction and Watermark Retrieval

Shares Creation Based Scheme

The main drawback of this technique is that it alters the original image in order to embed the shares, and the extraction procedure adds to the calculation cost. Some research has therefore been conducted to use the advantages of *VC* more judiciously. The schemes that generate an additional share to authenticate the image instead of embedding the share in the cover images, are addressed here. The conceptual model of share creation and copyright verification is shown in Figures 2.3 and 2.4.

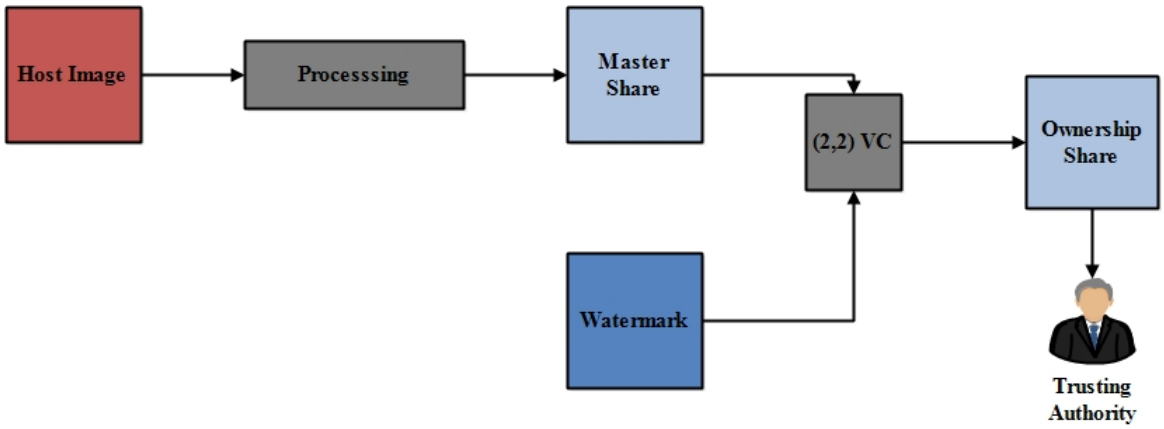


Figure 2.3: Spatial Domain Based Schemes - Share Creation Phase

Hwang (2000) suggested the first digital watermarking scheme using *(2,2)-VC*, where the host image is not altered as no share is embedded into it. Instead, a share is created from the original host image referred to as *MS*. This *MS* together with the watermark is used to construct *OS*, which is stored with *TA*. The watermark is then recovered by superimposing these shares on over of each

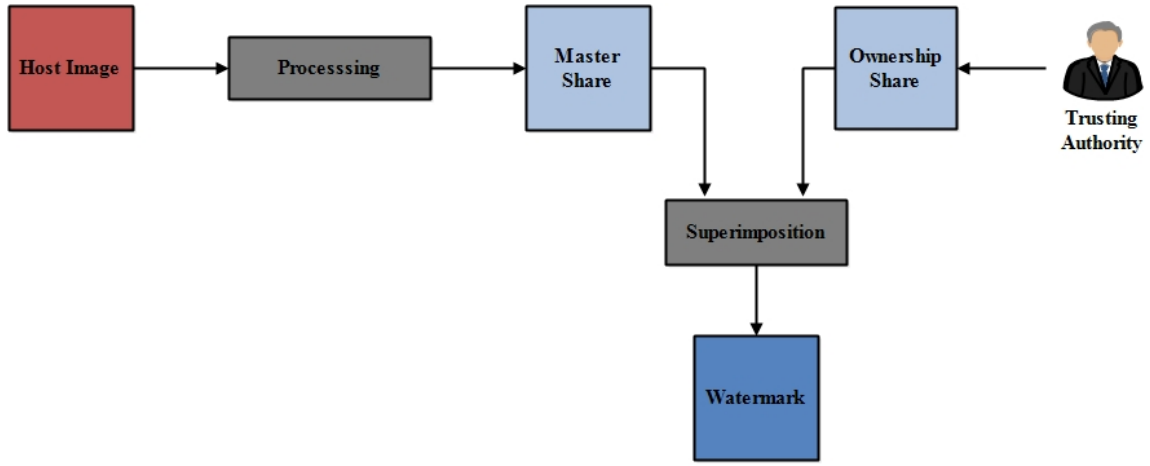


Figure 2.4: Spatial Domain Based Schemes - Copyright Proving Phase

other. This watermark is used to verify the host image's copyright. This technique has proven to be resistant to a variety of attacks.

Wang et al. (2000) imposed specific emphasis on robustness against cropping attacks in their proposed scheme. This scheme repeats the watermark around the image multiple times, depending on their sizes, to deal with the image cropping attacks. The watermark is divided into public watermark and private watermark using the *VC* system. The public watermark is embedded in the edge blocks of the host image. The outcomes of the simulation indicate that the scheme can withstand a range of image processing attacks and exhibit higher robustness for the cropping attack compared to the existing schemes. The key limitation to this scheme is that the host image is modified by embedding a watermark.

Chang et al. (2002) used Torus Automorphism to extend Hwang (2000) scheme. This scheme has the same benefit as no pixels in the host picture are altered. This scheme often appears to be robust to a variety of attacks. However, the size of the watermark is constrained by the size of the host image and the robustness of the JPEG compression ratio decreases.

Hou (2002) proposed a copyright protection scheme wherein *MS* is generated using the highest bit-plane of the host image. The share size is double the size of the host image, which is a major disadvantage of this technique.

These schemes had the potential to include a single watermark in the host image. This potential was improved by Hsu and Hou (2005) in their proposed novel copyright protection scheme based on *VC* and statistics by including multiple watermarks. This scheme is capable of embedding multiple watermarks without altering the host image and has the potential to verify the ownership of the image without the need of the original image. The additional benefit of the scheme is that

there is no constraint on the size of the host image. The scheme used Sampling Distribution of Means (SDM) to generate the share from the host image, which helped in ensuring robustness and unambiguity. This scheme can be extended to the gray scale and the color images. However, this scheme demonstrates vulnerability to some of the image manipulation attacks, such as sharpening, noise addition and JPEG compression. Furthermore, the shares and restored images are four times larger than the host image.

Wang and Chen (2007) proposed a blind watermarking scheme based on *VC* and Singular Value Decomposition (SVD). Here, the image is divided into equivalent size blocks and *SVD* is applied to these blocks. The largest single value of each component is compared to the mean of all the largest single values used to construct a binary map that is used to construct *MS*. This *MS* is often used with the watermark to build *OS*.

Hou and Huang (2012) suggested a copyright protection scheme to improve the limitations of Hsu and Hou (2005). They generate unexpanded shares using the law of large numbers by comparing randomly selected pixel pairs. Nevertheless, the scheme proves to be vulnerable in some instances when images are attacked by certain image processing attacks.The pixel values in either pair can alter during attacks, resulting in a range of consequences when retrieving the watermark.

2.1.2 Frequency Domain Features Based

All these schemes listed are based on spatial domain. Spatial domain schemes are very vulnerable to image processing attacks. In these systems, pixel values in the spatial domain are transformed to amplitude coefficients in the frequency domain by means of different transformations. These coefficients are then used to construct *MS*. Such systems have been found to be more robust against image processing attacks. This section discusses frequency domain based copyright protection schemes. Here, the shares are generated using the frequency components of image. These schemes can be divided into two categories depending on the number of image owners: Single Owner Schemes and Multiple Owner Schemes.

Schemes for Images with Single Owners

The copyright protection schemes where the images are owned by a single owner are discussed here. The basic structure of share creation and copyright proving is shown in Figures 2.5 and 2.6.

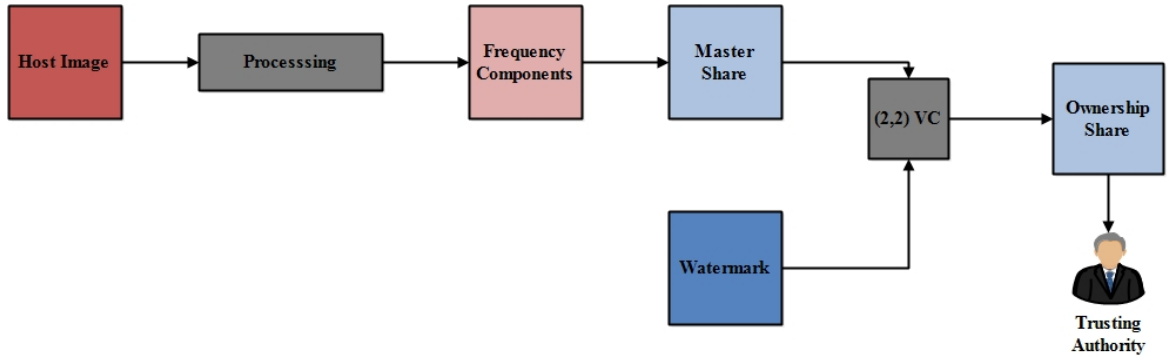


Figure 2.5: Frequency Domain Features Based Schemes - Share Creation Phase

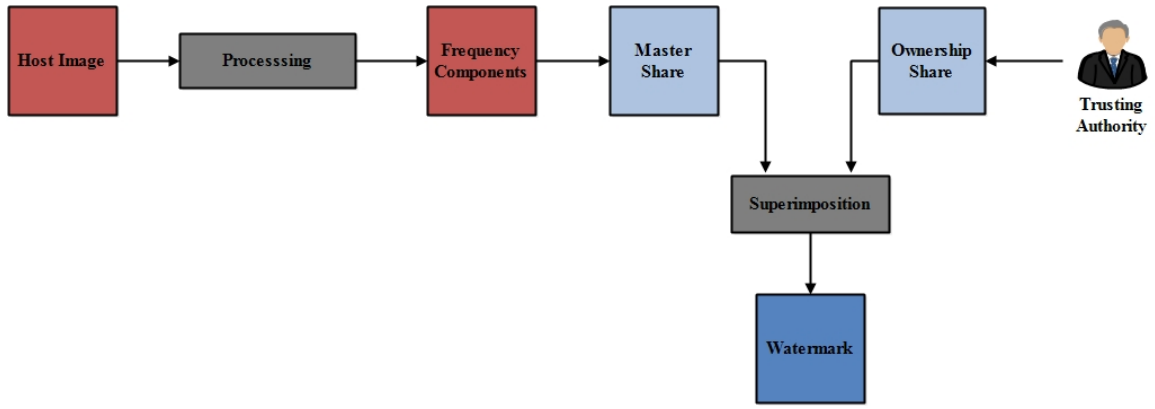


Figure 2.6: Frequency Domain Features Based Schemes - Copyright Verification Phase

Hsieh et al. (2005) proposed yet another copyright protection scheme, this time focusing on weather satellite images. This scheme generates *MS* by extracting features from every 4×4 neighbourhood in lower sub-band coefficients by applying Discrete Wavelet Transform (DWT) to the host image. This scheme showed better robustness than the existing schemes. The pixels of the host image are not modified in this scheme, and thus are seen to be of interest to unchangeable weather satellite images. Using grey level slicing, a cloud image is created from the host image in this scheme. A sampling plane is created using original and cloud image that is processed by applying two-level DWT. The scheme used *VC* and Torus automorphism to create shares from the host image, which ensured security. The experimental results demonstrate the robustness of the system with an accuracy rate greater than 85%.

Another copyright protection scheme based on *DWT* and *VC* was proposed by Lou et al. (2007). Using the secret key and the relationship between the low and middle sub-band *DWT* coefficients, the *MS* is created in this scheme. *OS* is developed using *MS* and a watermark image by using a codebook. The *XOR* operation is performed between *MS* and *OS* to retrieve the watermark. The scheme displays strong robustness in the against multiple attacks. However, the false positive rate

is very high, *i.e.* using the secret key, the watermark can be obtained even from other unprotected host images. (Chen et al. (2009)).

Wang and Chen (2009) proposed a hybrid copyright protection scheme based on *DWT*, *SVD* and *VC*. In this scheme, two-level *DWT* is applied to the host image and random pixel locations are chosen from the LL2 sub-band using *Pseudo Random Number Generataor (PRNG)*. Then *SVD* is applied to blocks centered at the specified pixel location to generate a collection of singular values. Using *k*-means clustering, the first half of these discrete values are split into two clusters. The *MS* is constructed using the binary map obtained from the clustering result. The system proves to be secure and robust against common attacks on image processing.

Based on Fractional Fourier Transform (FrFT) and *VC*, Rawat and Raman (2012) presented another robust and blind watermarking approach. The image is segmented into $4times$4non-overlapping blocks in this approach. Using PRNG, a set of blocks are chosen that are converted using *FrFT* and *SVD*. A matrix is generated using the largest single value of each element. This matrix is used to create *MS*, which is combined with the watermark to construct *OS*. *FrFT* helps to ensure security, since watermark can not be retrieved if the *FrFT* orders are unknown to the attacker. In terms of robustness, the method outperformed the previous ones, especially when it came to rotation and resizing attacks.

Wu and Sun (2013a) developed an image watermarking scheme based on Discrete Cosine Transform (DCT) and *SVD*. In this scheme, the host image is divided into alternating blocks which are further transformed using *DCT*. *SVD* is applied on randomly selected transformed coefficients and *MS* is generated from the *SVD* diagonal matrix. *XOR* operation between *MS* and watermark is used to create *OS*.

Benyoussef et al. (2013) proposed using the dual tree complex wavelet transform to construct a share that is embedded in the LL sub-band as a copyright protection mechanism. This scheme has been extended by them to propose the schemes for medical images (Benyoussef et al. (2014)) and videos (Benyoussef et al. (2015)).

Another robust copyright protection strategy based on *DWT* and the law of large numbers was introduced by Hou et al. (2016). Devi et al. (2016) introduced a secure and robust copyright protection scheme based on *DWT* and *SVD* to provide better robustness. In order to improve robustness of the existing schemes, Shao et al. (2016) used Quaternion-type moment invariants to create *MSs* in their scheme. Xue et al. (2019) proposed an image authentication scheme based on Scale In-

variant Feature Transform (SIFT) key points, in which a hash key is generated by combining *LBP* characteristics and *SIFT* key points hidden in the host image. Fatahbeygi and Tab (2019) introduced an image watermarking strategy by constructing a *MS* employing canny edge detection and support vector machine. Except for rotation, this design improved resistance to various attacks and suffered from pixel expansion.

Makbol et al. (2016) proposed a robust hybrid block picture watermarking scheme related on the characteristics of *DWT*, *SVD* and *Human Visual System (HVS)*. In this scheme, the original image is decomposed into 8×8 non-overlapping blocks. The blocks with the lowest edge entropy values are then chosen as the strongest embedding regions. *SVD* is applied to the LL subband of first level *DWT* to modify some of the elements in its U matrix.

Ali et al. (2018) proposed a watermarking scheme based on *DWT*, *SVD*, *FrFT* and *VC*. *DWT* and *FrFT* are applied to the host image to obtain an invariant domain. To insert a watermark image, the random location of the *FrFT* matrix is chosen. The largest singular values corresponding to the most conceptually significant regions in the image are chosen as reliable features,that are used to create the *MS*. Finally, *OS* is created from the *MS* and the watermark image.

Multiple Owner Schemes

The schemes discussed in the preceding sections are only applicable to single images. For VC-based watermarking techniques, applications involving numerous cover images with numerous owners have not received much attention. The copyright protection strategies for photographs with numerous owners are discussed in this section. The basic structure of share creation and copyright proving is shown in Figures 2.7 and 2.8.

Liu and Wu (2011) presented a watermarking strategy based on *VC* and *DWT* that works for numerous cover images with multiple owners. To build feature shares, two level *DWT* is applied to the cover images in this scheme. Every owner is given a set of shares that appear to be noisy and random. A secret share is created using feature shares, the key, and the watermark, and it is stored and registered with the *TA*. When the need to verify ownership of attacked photos occurs, the watermark is retrieved using the *XOR* operation, which superimposes the secret share, feature shares, and keys from each owner. Chaos, torus automorphism, and noise reduction techniques are used to improve the scheme's robustness. Except for rotation, the technique is said to be secure and robust against a variety of image processing attacks. The size of the watermark is also deter-

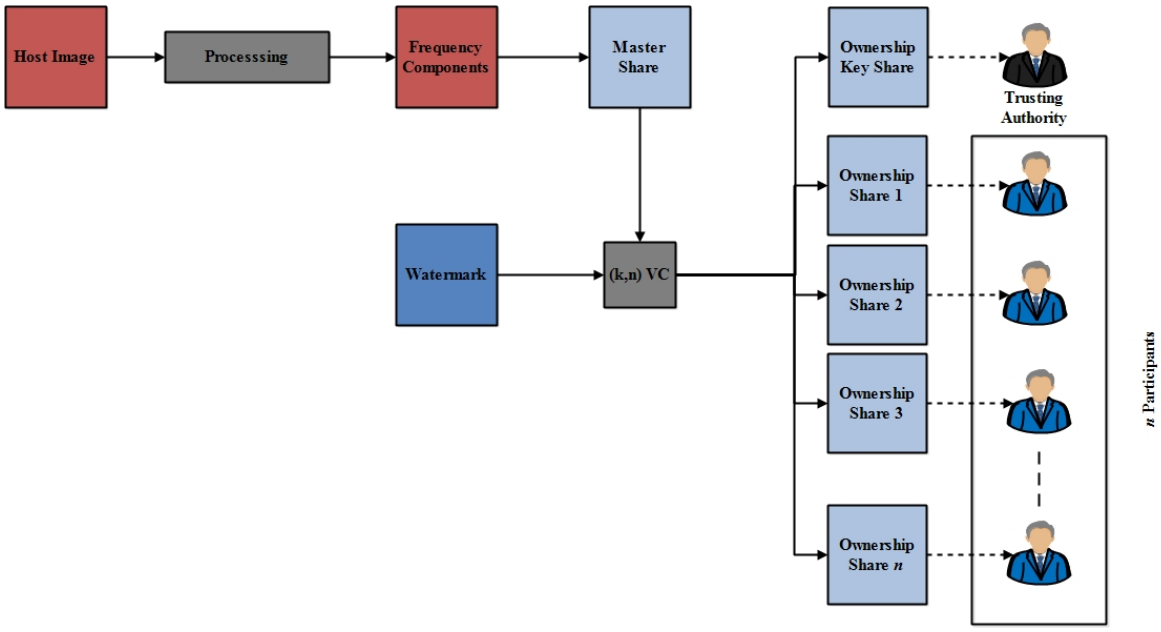


Figure 2.7: Frequency Domain Features Based Schemes for Multiple Owners- Share Creation Phase

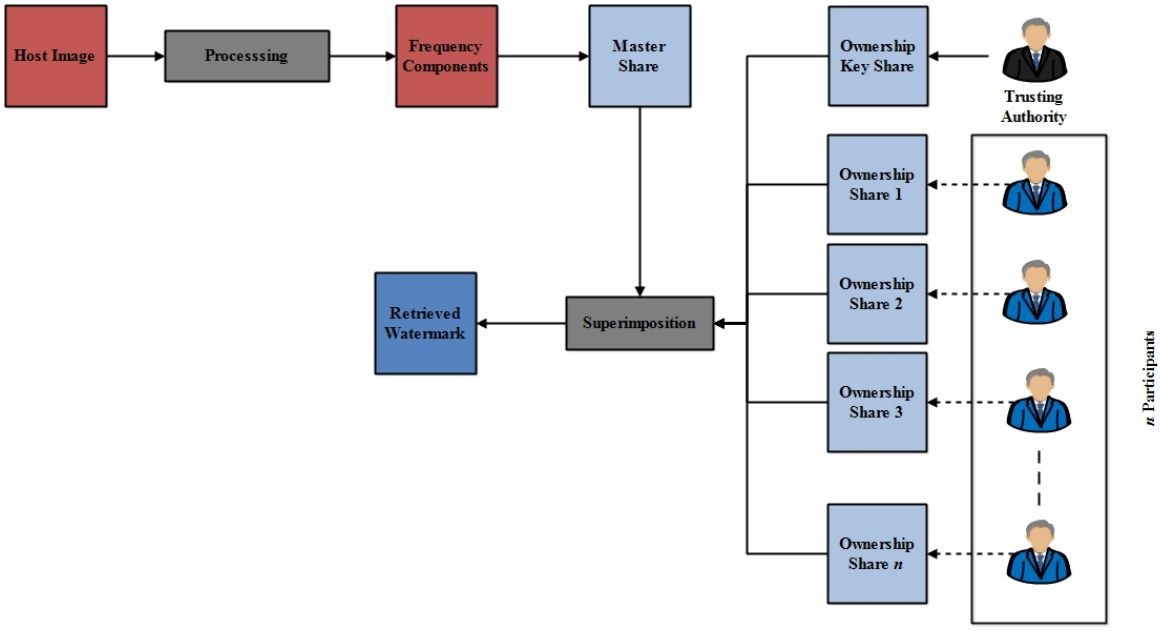


Figure 2.8: Frequency Domain Features Based Schemes for Multiple Owners- Share Creation Phase

mined by the size of the cover images. Amiri and Moghaddam (2016) improves on this technique by employing a pseudo random generator and *SIFT* to generate feature shares. In addition, the size of the watermark is independent of the size of the cover image. As side information, the pseudo random generator key and the *SIFT* key points required for watermark extraction are recorded and communicated. For multiple images, this approach succeeded, but not for multiple owners.

Table 2.1: Summary of VC based Copyright Protection Schemes

Scheme	MS Construction	Type of Shares	Pixel Expansion	Watermark Retrieval	VC Type	No.of Participants	No.Of Images	Image Type	False Positives
Hou and Chen (2000)	Spatial Domain	Meaningless	Yes	Extraction	(2,2)	1	1	Grayscale	
Hwang (2000)	DWT	Meaningless	Yes	OR Superimposition	(2,2)	1	1	Grayscale	Yes
Chang et al. (2002)	Torus Automorphism	Meaningless	Yes	OR Superimposition	(2,2)	1	1	Grayscale	
Hou (2002)	Highest Bit Plane of Image	Meaningless	Yes	OR Superimposition	(2,2)	1	1	Grayscale	
Hsu and Hou (2005)	SDM	Meaningless	Yes	OR Superimposition	(2,2)	1	n	Grayscale	
Wang and Chen (2007)	SVD	Meaningless	Yes	OR Superimposition	(2,2)	1	1	Grayscale	

Table 2.1 Continued..

Scheme	MS Construction	Type of Shares	Pixel Expansion	Watermark Retrieval	VC Type	No.of Participants	No.Of Images	Image Type	False Positives
Hou and Huang (2012)	Law of Large Numbers	Meaningless	Yes	OR Superimposition	(2,2)	1	1	Grayscale	
Hsieh et al. (2005)	DWT, Torus Automorphism	Meaningless	Yes	OR Superimposition	(2,2)	1	1	Grayscale	
Lou et al. (2007)	DWT	Meaningless	Yes	XOR Superimposition	(2,2)	1	1	Grayscale	Yes
Wang and Chen (2009)	DWT, SVD, K-means Clustering	Meaningless	Yes	OR Superimposition	(2,2)	1	1	Grayscale	
Liu and Wu (2011)	DWT, Torus Automorphism	Meaningless	No	XOR Superimposition	(k,n)	k	n	Grayscale	

Table 2.1 Continued..

Scheme	MS Construction	Type of Shares	Pixel Expansion	Watermark Retrieval	VC Type	No.of Participants	No.Of Images	Image Type	False Positives
Rawat and Raman (2012)	FrFT, SVD	Meaningless	Yes	OR Superimposition	(2,2)	1	1	Grayscale	
Wu and Sun (2013b)	DCT, SVD	Meaningless	Yes	OR Superimposition	(2,2)	1	1	Grayscale	
Hou et al. (2016)	DWT, Law of Large Numbers	Meaningless	No	OR Superimposition	(2,2)	1	1	Grayscale	
Devi et al. (2016)	DWT, SVD	Meaningless	Yes	OR Superimposition	(2,2)	1	1	Grayscale	
Shao et al. (2016)	Quaternion-type moment invariants	Meaningless	Yes	OR Superimposition	(2,2)	1	1	Grayscale	
Xue et al. (2019)	SIFT, LBP	Meaningless	No	Extraction	(2,2)	1	1	Grayscale	

Table 2.1 Continued..

Scheme	MS Construction	Type of Shares	Pixel Expansion	Watermark Retrieval	VC Type	No.of Participants	No.Of Images	Image Type	False Positives
Fatahbeygi and Tab (2019)	Canny Edge Detector, SVM	Meaningless	No	OR Superimposition	(2,2)	1	1	Grayscale	
Ali et al. (2018)	DWT, SVD, FrFT	Meaningless	Yes	OR Superimposition	(2,2)	1	1	Grayscale	
Amiri and Moghaddam (2016)	DWT, SVD, SIFT	Meaningless	No	XOR Superimposition	(2,n)	1	n	Grayscale	

2.2 Authentication Schemes with VC

Various secret sharing schemes have been proposed which also incorporate authentication. In such schemes, the shares are constructed from the secret image, and then these shares along with the authentication bits are hidden inside the cover image which is supposed to be transferred through the communication channels. These authentication code bits are employed on the receiver side to confirm the authenticity of the marked images received.

2.2.1 Embedding Based Schemes

Lin and Tsai (2004) proposed a VC scheme which had authentication capability also. The shares for the secret image are generated in this scheme, and then these shares, along with the appropriate authentication codes, are inserted into the cover image. The share bits and one authentication bit are inserted in a $2x2$ block of the cover picture using Least Significant Bit (LSB) substitution, *i.e.* 8 bits of each pixel in the created shares and one authentication bit. The image is later verified when the authentication codes are extracted from the image. However, size of the cover image increases to four times the secret image's size. Parity bits are used in this scheme for authentication, though they offer weak authentication and polynomial based VC has been used to generate the shares.

Yang et al. (2007) modified Lin and Tsai (2004) to prevent cheating by its participants. This scheme also used polynomial based VC to generate the n shares, but unlike the previous scheme (Lin and Tsai (2004)) which set the value of the variable p to 251, in this scheme value of p is set to the Galois Field (GF), *i.e.* $p = g(x) = x^8 + x^4 + x^3 + x^1 + x^0$, which reduces the distortion in the received secret image. They used Hash-based Message Authentication Code to solve the dishonest problem by rearranging the arrangement of the nine bits in the $2times2$ block, resulting in a superior visual quality stego-image. The scheme's capacity to authenticate and the quality of the rebuilt image were both improved. The advantage of the scheme was that it can retrieve the secret image back with minimum distortion, but the cover image still remains four times the size of secret image and also it can authenticate fake images successfully sometimes. The image quality in Yang et al. (2007) scheme was enhanced by Wu et al. (2008) who proposed an authentication scheme based on LSB substitution and optimal pixel adjustment.

Chang et al. (2008) proposed another VC scheme which used Chinese Remainder Theorem (CRT) for authentication which improved the authentication ability but the issue of pixel expansion

still existed. The size of the cover image was relatively decreased as compared to the previous two schemes but it was still twice the secret image's size. As this scheme used CRT to evaluate the authentication bits, the computational complexity got increased.

The described schemes were able to detect and verify if the marked image received has been tampered or not, but none of them had the ability to repair the tampered areas. This weakness was worked upon by Chang et al. (2011) whose scheme could repair the inauthentic area in the received secret image to ensure that the information can be retrieved successfully even from the tampered secret images. The PSNR of the stego image is assures to be more than 45 dB, so that the original information can be recognized by the authorized parties..

Another scheme was proposed by Lou et al. (2011) in which the secret image is embedded inside two meaningful cover images, with no pixel expansion and larger embedding capacity at the same transmission cost and better contrast. This VC scheme generated meaningful share images and was used as an authentication scheme.

Eslami and Ahmadabadi (2011) proposed a scheme in which new embedding scheme is proposed such that the size of the block depends on the data to be hidden , hence the cover images are used efficiently for hiding the data. This scheme also included an authentication-chaining method which used two authentication bits and was able to achieve 15/16 tamper detection ability. All the bits of the cover image were used to hide the data and authentication bits were increased as it used authentication-chaining method. But its disadvantage was even if a single block was modified intentionally or unintentionally, the authentication fails for the rest of the image. The authentication abilities for the increased block sizes were improved and the individual blocks of the stego image could also be authenticated in Ulutas et al. (2013). In this scheme, authentication strength depending on block size is proposed. Four bits per block are used for authentication but it can be increased with the increase in block size. The authentication bits for the current block are inserted in the next block. Thus, unlike Eslami and Ahmadabadi (2011) transmission error that claims an authentic block as fake block affects only the former block. The visual quality of the stego images was also better as compared to the existing ones and could authenticate the rest of the stego image after encountering an altered block in the stego image.

Unlike the mentioned schemes, Yang et al. (2012) proposed an authentication scheme that did not require any parity bits and provided higher detection ratio. This scheme is based on bivariate polynomial that helps in combining both authentication and secret sharing features into the share

bits without using any additional authentication bits.

Another VC scheme with authentication abilities, which could share meaningful shares, using the concepts of CA, DWT and hash functions, was proposed by Wu and Sun (2013b). This scheme could successfully verify if the received images are tampered or not, would repair the damaged areas with the help of the hidden information but did not had abilities to recover the secret information from the tampered image.This scheme showed low computational cost, good remedy abilities against tampering , cropping and other attacks and also good tamper detection rate.

Steganalysis techniques can easily discover the stated techniques that were based on LSB substitution. This issue was addressed by Zarepour-Ahmadabadi et al. (2016) and modified. This scheme enhanced the visual quality of images and provided adaptive authentication ability. The authentication bits are generated in such a way that if one block gets tampered, it affects more than one block. The LSB is replaced with blockwise XOR that helps in withstanding steganalysis attacks. Also the scheme is flexible for secret and cover images of different sizes, as block size is decided dynamically.

All of these schemes had a secret leakage problem. The polynomial in this case is a linear transformation with k=2, establishing a linear relation between the generated share and the secret image. One of the shares may reveal only a portion of the image's content. As a result, when the shares are included in cover images, third-party attackers have access to a portion of the hidden image's content. Additionally, the embedding capacity and visual quality must be improved.

Most of the these schemes work for uncompressed images only. Also, these schemes do not have abilities to recover the tampered image. To address these issues, Wu and Yang (2019) proposed a threshold partial reversible absolute moment block truncation coding authentication technique. Under GF-28, the secret image is partitioned into n shares using a polynomial. Using proposed embedding techniques, the created shares are inserted into cover images to create meaningful shares. The scheme has the ability to partially recover the tampered images.

There were also some VC-based authentication techniques based on reference matrix proposed. Chang et al. (2010) presented a reversibility-based Secret Image Sharing (SIS) approach for Sudoku. A reference matrix equal to the hidden image size is generated using grids of size $16x16$. The value of each pixel pair in the cover image is determined by the coordinates of the reference matrix. When the pixel pair value and the shadow's shared pixels replace the polynomial's coefficients, a set of shadows is created. The scheme recovers data without loss and uses the same payload, but it fails

to detect fraud. Furthermore, transmitting the mapping table adds to the overall transmission cost. Later, the Sudoku matrix is replaced with a turtle shell matrix Liu et al. (2018), with extra authentication capabilities to identify altered image regions. Because the transferred value is recorded in each polynomial, these techniques were applied to a single cover image. As a result, the schemes aren't used on multiple cover images.

To handle the security concerns of meaningless shares, the shares are embedded into the cover image to give an illusion that some meaningful content is being shared. Most of the previous schemes used LSB replacement to embed data. Xiong et al. (2020) proposed a secure and effective DWT based secret image sharing with authentication. They improved the embedding capacity as well as the visual quality. The scheme has the capabilities to detect whether the share is forged or not. Using permutation and a key, the scheme also avoids secret leakage. Embedding a greater number of authentication bits improved authentication ability. Inspite of all the advancements, there is still a scope to enhance the detection ratio in this scheme. Also, the images could not be recovered after being tampered.

2.2.2 Share Creation Based Scheme

Most of the discussed schemes use hash functions and information hiding that leads to high recovery complexity. The shares and authentication data need to be extracted from the marked images to prove the copyright. Hence, some schemes were proposed that used an additional share to authenticate the image instead of embedding the shares inside the cover images. These schemes create meaningful shares from the watermark and cover images using the properties of VC.

The Two in One Secret Sharing Schemes(Sridhar and Baskaran (2015); Li et al. (2012)) that combined the benefits of traditional VC and Polynomial based VC lacked authentication of image and shares being constructed. This was improved upon by Srividhya et al. (2016) by creating meaningful shadows and enhancing its security by sharing an authentication share along with the secret image. They created an additional authentication share that consisted of authentication information which helped in detecting if the received host image is tampered.

Another scheme on similar grounds was proposed by Liu et al. (2018) shows low accuracy in detection of fake participant and the recovery is lossy. Yang et al. (2020) proposed an authentication scheme that uses an additional share instead of information hiding by using polynomial based VC.

This scheme shows low computational complexity at the time of authentication detection, has zero pixel expansion and lossless recovery.

Table 2.2: Summary of VC based Authentication Schemes

Scheme	Embedding	Pixel Expansion	Recover Ability	Highest DR
Lin and Tsai (2004)	Yes	Yes	No	-
Yang et al. (2007)	Yes	Yes	No	-
Wu et al. (2008)	Yes	Yes	No	-
Chang et al. (2008)	Yes	Yes	No	$\frac{15}{16}$
Chang et al. (2011)	Yes	Yes	Partially	$\frac{15}{16}$
Lou et al. (2011)	Yes	No	No	-
Eslami and Ahmadabadi (2011)	Yes	Yes	No	$\frac{255}{256}$
Ulutas et al. (2013)	Yes	Yes	No	0.9
Yang et al. (2012)	Yes	Yes	No	-
Wu and Sun (2013b)	Yes	Yes	No	$\frac{255}{256}$
Zarepour-Ahmadabadi et al. (2016)	Yes	Yes	No	-
Wu and Yang (2019)	Yes	Yes	Partially	-
Xiong et al. (2020)	Yes	No	No	$1-\frac{1}{2^{160}}$
Srividhya et al. (2016)	No	Yes	No	-
Liu et al. (2018)	No	Yes	Lossy	-
Yang et al. (2020)	No	No	Partial	-

2.3 Gaps

In context to the literature review conducted on the existing Copyright Protection and Authentication schemes on images using VC and Watermarking, following gaps have been found out, as listed below:

- Existing copyright protection and authentication schemes based on VC and Watermarking generate only meaningless random shares for the watermark, which lead to lesser security, as the random looking shares raise suspicions that secret information is being stored or trans-

mitted.

- Most of the existing copyright protection schemes suffer from pixel expansion in the shares generated for the watermark, which results in larger storage and transmission cost and also loss in contrast.

- The existing copyright protection schemes based on VC and watermarking use *(2,2)*-VC which leads to some gaps in security and robustness of the scheme, as in that case only one participant is involved, and in the case of failure, the watermark cannot be retrieved back if the share with the participant is lost or damaged.

- The existing copyright protection schemes have low PSNR for the attacked host images and NC of the extracted watermark from the attacked images.

- The existing secret image sharing with authentication schemes suffer from pixel expansion, low visual quality of the reconstructed secret image and low detection ratio.

- Copyright Protection schemes based on VC and watermarking, using multiple watermarks to protect the cover image for multiple hosts have not been studied much.

- Color images have not been much studied for the copyright protection and authentication using VC and Watermarking, as most of them work on binary and grayscale images.

2.4 Objectives

On the basis of gaps identified from the literature review, following objectives are proposed.

- To study and analyze the existing Copyright Protection and Authentication Schemes using Visual Secret Sharing schemes.

- To develop robust Copyright Protection Scheme(s) for digital images with Visual Secret Sharing schemes.

- To develop improved Authentication Scheme(s) for digital images with Visual Secret Sharing schemes.

- To compare the designed schemes with the existing schemes.

CHAPTER 3

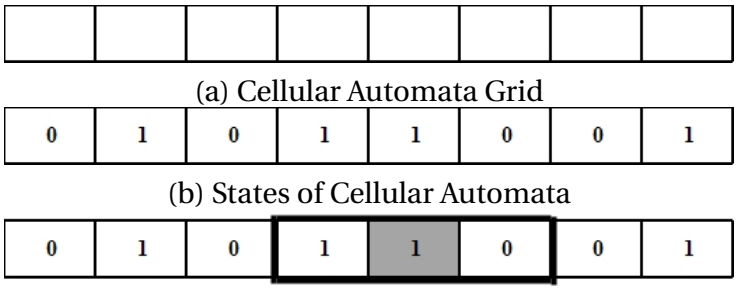
Cellular Automata based Image Authentication Scheme using Wavelet Packet Transform

.

3.1 Introduction

Most of the *VC* based image authentication schemes hide the share and authentication data into the cover images by using an additional data hiding process. This process increases the computational cost of the schemes. Pixel expansion, meaningless shares and use of codebook are other challenges in these schemes. To overcome these issues, an authentication scheme is proposed in which embedding into the cover images is not required. This makes the scheme completely imperceptible. This scheme creates meaningful authentication shares are created using the watermark and cover

Contents of the work presented in this Chapter have been published in *Computing and Informatics*, Vol. 38, pp. 1272-1300, 2019. (SCI Indexed)



(a) Cellular Automata Grid

(b) States of Cellular Automata

(c) Neighborhood of a cell

Figure 3.1: Representation of CA

images. The meaningful authentication shares help in enhancing the security of the scheme while size invariance saves transmission and storage cost. The watermark can be retrieved just by superimposing these authentication shares, thus reducing the computational complexity at receiver's side. The scheme possesses the ability of tamper detection. Experimental results demonstrate the improved security and quality of the generated shares of the proposed scheme as compared to existing schemes.

3.2 Background

In this section *CA* and *WPD* are discussed, which are used in the proposed scheme.

3.2.1 Cellular Automata

CA is an array of entities which are known as cells. Every cell has a finite state having value either 0 or 1. Every cell has a neighborhood, which is usually described by its adjacent cells. The cells of the *CA* exhibit following properties:

- **Grid:** All cells of *CA* arrange themselves in the form of a grid, as shown in Figure 3.1-(a).
- **State:** Every cell has a state. The number of state possibilities is typically finite. Every cell usually has 2 states: (0 and 1) or (ON and OFF) or (ALIVE and DEAD), as shown in Figure 3.1-(b).
- **Neighborhood:** Neighborhood involves the cell and its adjacent cells, as shown in Figure 3.1-(c).

The state of the cell at an instant of time *t*, depends on its state at time *t*-1 along with the state of

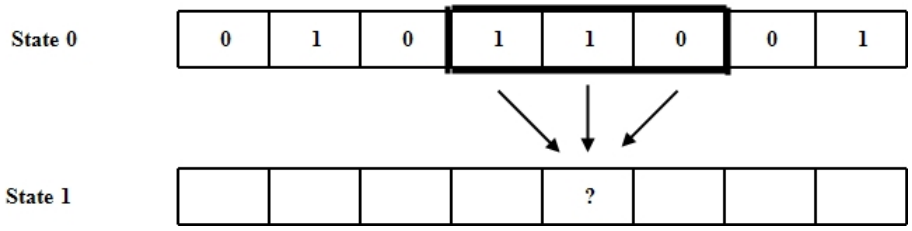


Figure 3.2: Transition of a cell from one state to next state

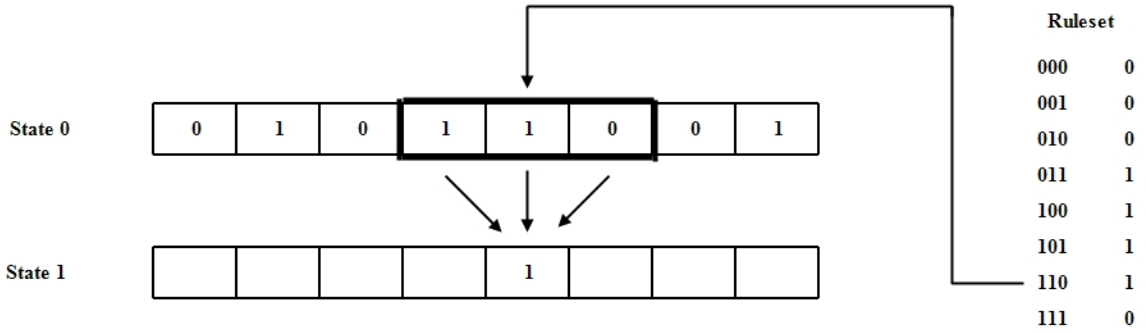


Figure 3.3: Use of Rule 30 to generate next state

its neighbors at time t-1. A certain set of rules is followed to determine this current state of the cell on the basis of the previous states of the cell and its neighbors. This can be written as:

$$S(t) = F(S(t-1))$$

where $S(t)$ represents state of a cell at time t. Function F is determined by various rules described in Yampolskiy et al. (2014). This has been described in Figure 3.2.

The state configuration for every cell along with its right and left neighborhood, is represented by three bits. *e.g. 100*. Hence there are total eight possible neighborhood state configurations. Thus the rulesets are represented by eight bits *e.g. Rule 10001010*, representing eight different state configurations. In the proposed scheme Rule 30 has been used. Generation of new state from the previous state using Rule 30 is shown in Figure 3.3.

In terms of a Wolfram elementary *CA*, there are 256 possible rulesets. The ruleset used here is commonly referred to as Rule 30 because if the binary sequence 00011110 is converted to a decimal number, integer 30 is obtained. The generic *CA* is extended to two dimensions Yampolskiy et al. (2014) which permits direct comparisons to real physical systems like crystal growth, chemical reaction-diffusion systems, simulation of turbulent flow patterns, *etc.* Two Dimensional *CA* supports variety of lattices and neighborhood structures like Von-Neumann neighborhood where the center cell is surrounded by four neighbors, Moore neighborhood that has eight neighbors around the center cell, *etc.*

Figure 3.4: Representation of different state configurations and their next states using Rule 30

Rule 30

Rule 30 is an one dimensional binary *CA* rule introduced by Wolfram (1983) in 1983. This rule has been used with VC in Yampolskiy et al. (2014). As stated in Ilachinski (2001), Rule 30 is an exceptional legal rule that is highly periodic and random. Hence, this rule is chosen in the proposed scheme helps in enhancing security. It has been described in Figure 3.4. The figure shows all eight possible state configurations and their corresponding next state. The color of the next state is determined by the color of the cell and its neighbors in the previous state. As the binary representation of the outcome of the rule turns out to be 30, the rule is known as Rule 30. ($30 = 00011110_2$)

3.2.2 Wavelet Packet Decomposition

WPD, also known as just Wavelet Packets is a wavelet transform where discrete-time sampled signal is passed through more filters as compared to the *DWT* Jensen and la Cour-Harbo (2001); Percival and Walden (2000). In *DWT*, every level is calculated by passing it only the previous wavelet approximation coefficients (low pass results) while in *WPD*, both detail (high pass results) and approximation coefficients are used to create the full binary tree.

The wavelet decomposition procedure splits the approximation coefficients into two parts. After splitting we obtain a vector of approximation coefficients and a vector of detail coefficients both at a coarser scale. The information lost between two successive approximations is captured in the detail coefficients. Then the new approximation coefficient vector is split again. In the wavelet packet approach, each detail coefficient vector is also decomposed into two parts as in approximation vector splitting. A pictorial representation of *WPD* over three levels is shown in Figure 3.5. *g[n]* is the low-pass approximation coefficients, *h[n]* is the high-pass detail coefficients.

For n levels of decomposition the *WPD* produces 2^n different sets of coefficients (or nodes) as opposed to $n+1$ sets for the DWT. However, due to the down sampling process the overall number of coefficients is still the same and there is no redundancy.

Wavelet Packets have a larger library of functions than wavelets, which helps in representing dif-

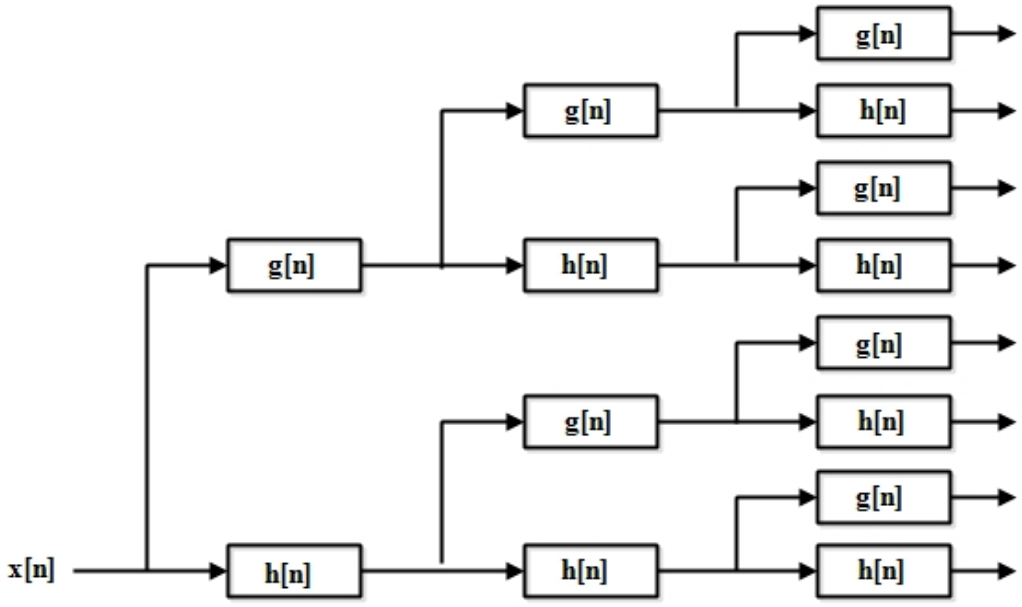


Figure 3.5: WPD over 3 levels (Jensen and la Cour-Harbo (2001))

.

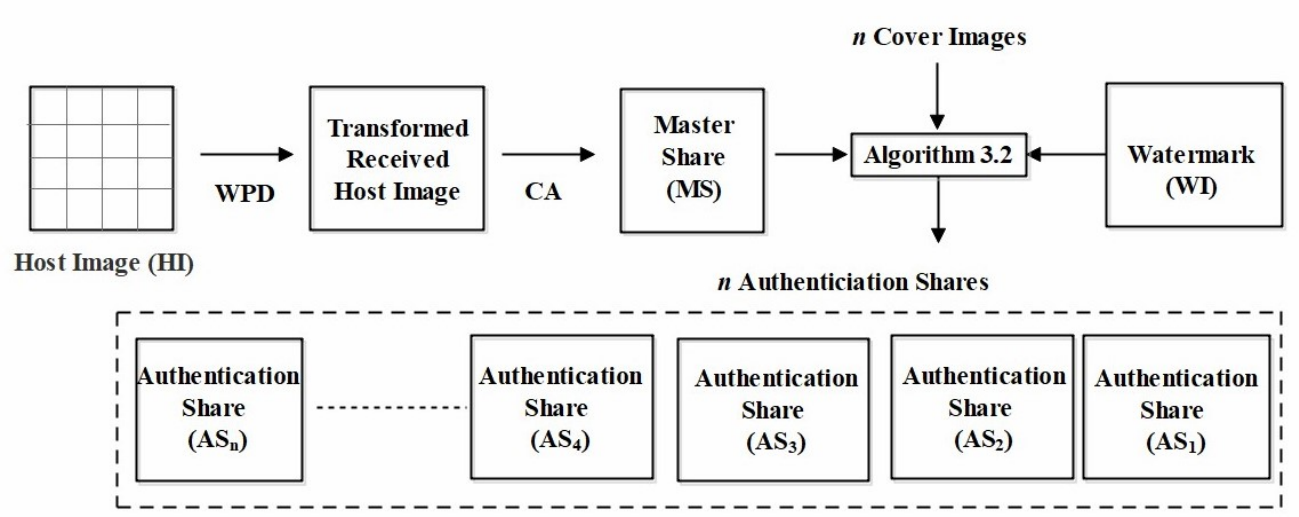
ferent types of images efficiently. Especially the images that have smaller scale wavelet coefficients and carry very little energy, can be effectively represented by *WPD*. Thus, in the proposed scheme we have utilized *WPD* to create a *MS* that contains maximum features of the image, else it might lead to increase in false positives and false negatives in the tamper detection cases.

3.3 Proposed Scheme

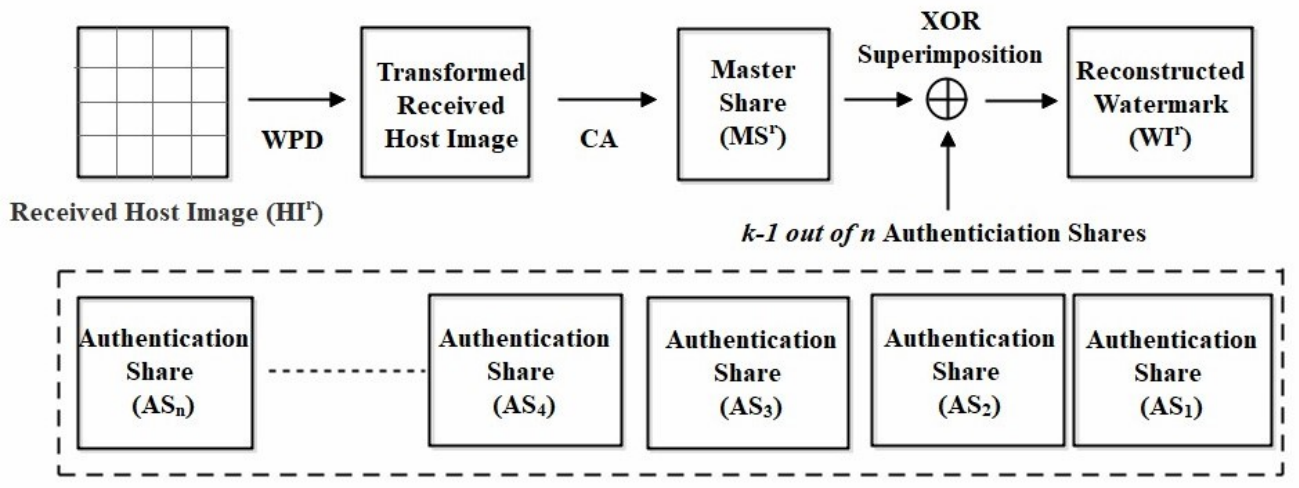
The proposed scheme consists of two phases: Share Generation Phase and Authentication Phase. It has been represented with the help of a block diagram shown in Figure 3.6.

3.3.1 Share Construction Phase

In the Share Construction Phase, *MS* is generated from the host image using *WPD* and *CA*. This phase is described in Algorithm 3.1. The Host Image is divided into equal sized blocks. A basis set is produced for every block by applying WPD. The binary code for the average value of this set is considered as the key for the respective block. The obtained key is used to generate the corresponding *MS* block using *CA* with Rule 30. Generation of *MS* has been explained with the help of an example in Figures 3.7 and 3.8. In Figure 3.7, a best basis set is constructed after applying WPD on an image block. The average of this set is calculated as 17. The binary conversion of 17 is considered as the key for CA, which is used to construct MS in Figure 3.8. The first row of the block is initialized with



(a)



(b)

Figure 3.6: Block Diagram of Proposed Scheme (a) Share Generation Phase (b) Authentication Phase

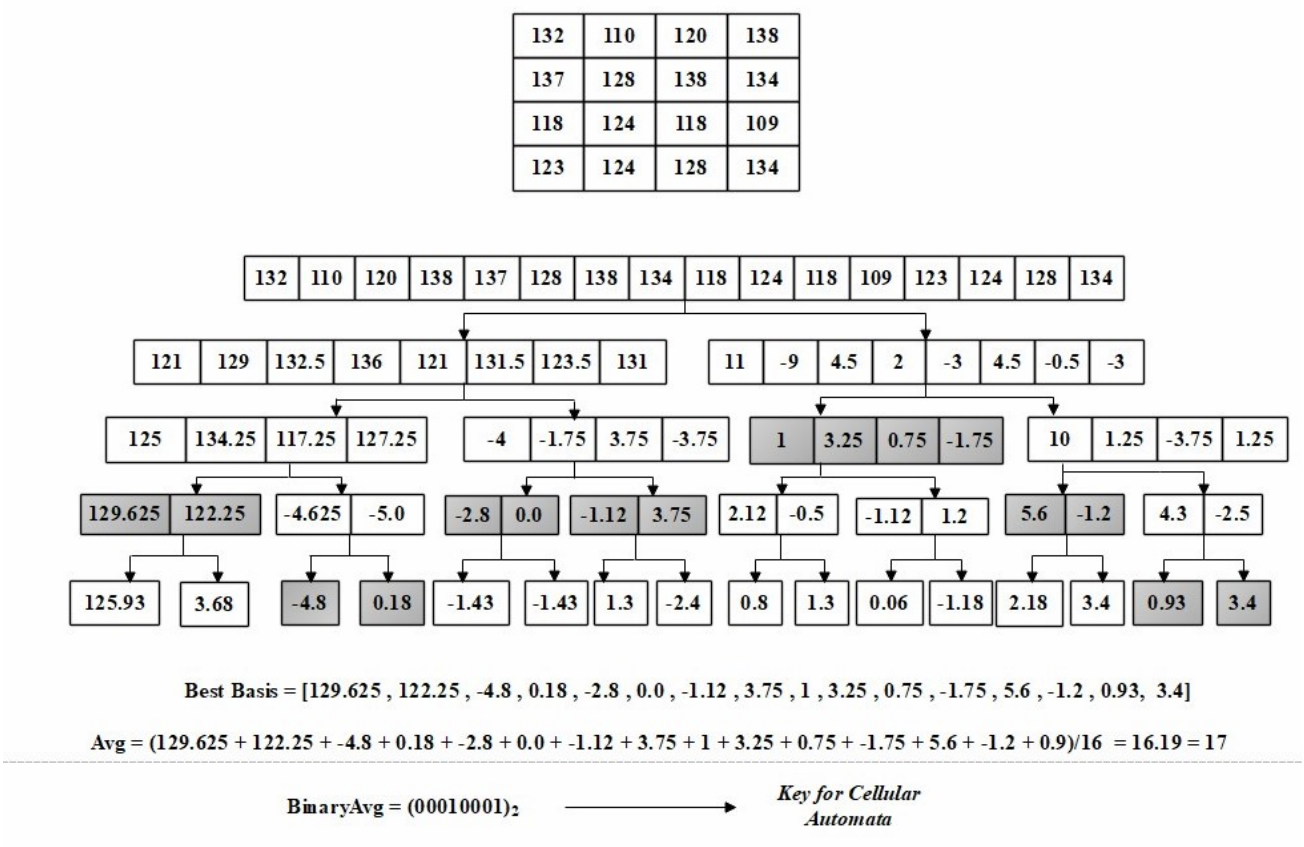


Figure 3.7: Example of WPD on SI Block of size 4 × 4

the key and the remaining rows are constructed from this first row using Rule 30.

Algorithm 3.1 MS Construction

Input: HI of size $hh \times hw$
Output: MS

Divide HI into equal size blocks HI_b of size $bh \times bw$, where $1 \leq b \leq nb$, $nb = \dfrac{hh \times hw}{bh \times bw}$
for every block (HI_b) **do**:
Apply WPD on HI_b and produce a best basis set.
Calculate average value Avg_b for the basis set
Convert Avg_b into 8 bit binary code $BinaryAvg_b$
Create corresponding MS by applying Rule 30 on $BinaryAvg_b$
Return MS

The benefits of using CA are that no codebook is required to create shares, no pixel expansion as every host image bit is represented by one bit in MS and no need to store the share as it can construct itself from its initial state. Existing VC scheme based on CA(Yampolskiy et al. (2014)) uses a key to generate the share. This key has to be transmitted from the sender to receiver as side information which results in additional transmission cost and can be accessed by third-party attackers too. While in the proposed scheme as a binary representation of mean for every block is considered as the key, there is no need to transmit the key as side information. It can be calculated by

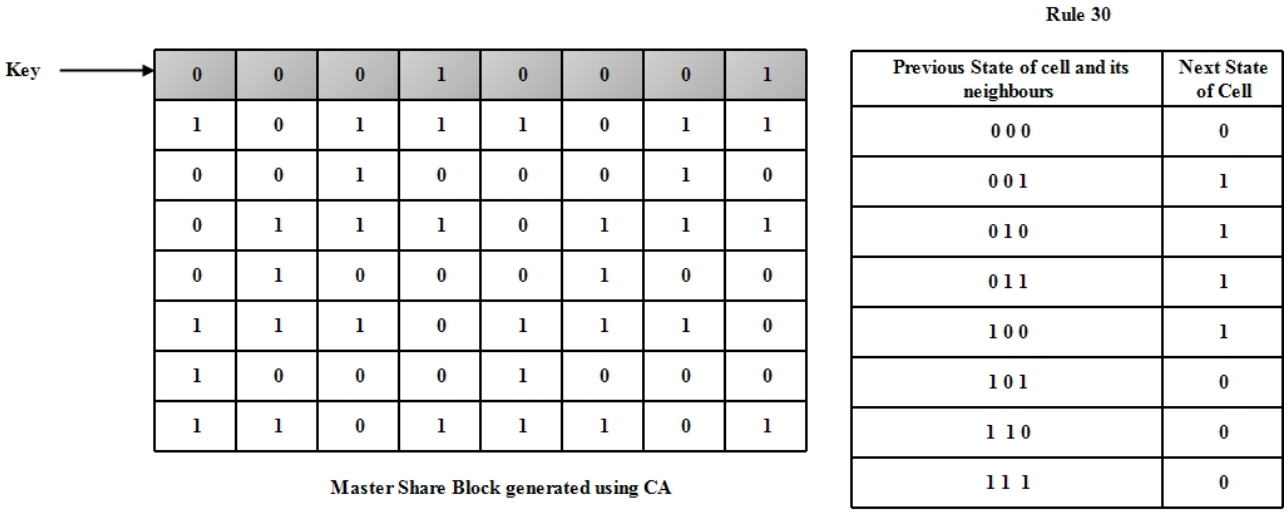


Figure 3.8: Generation of MS

the sender and receiver individually from their host and received image respectively. This reduces transmission cost and enhances security too.

After constructing MS, n meaningful and non-expanded authentication shares are generated using MS and WI. Generation of AS is illustrated in Figure 3.9. For every pixel, a random bit x is generated with probability p. If x turns out to be 0, pixel from watermark is included in the authentication share while if it turns out to be 1, pixel from cover image is included in the authentication share.

In proposed scheme, parameter p is set as a trade-off between visual quality of share images and WI' *i.e.*. The smaller value for p results into more visual-pleasing share images and lower image quality of retrieved watermark image, while the larger value for p results in less visual-pleasing share images and higher image quality of retrieved watermark image. The generated authentication shares $[AS_1, AS_2, ..., AS_n]$ are distributed among n participants and watermark is stored with a TA.

3.3.2 Authentication Phase

In this phase, the images are verified at the receiver's side, if they have been maliciously tampered. For the received host image HI', master share MS' is constructed using Algorithm 3.1 and authentication shares are retrieved from *k-1* participants. These *k-1* shares are superimposed with MS' to retrieve the watermark WI' using XOR operation. The superimposed result WI' should be similar to the WI stored with the TA. This similarity is compared using NHS. If the value of NHS tends towards

Algorithm 3.2 Authentication Shares Generation

Input: MS, *WI*, *n* CI $[CI_1, CI_2, ...CI_n]$ of size $ch \times cw$

Output: *n* Authentication Shares $[AS_1, AS_2, ..., AS_n]$

1: **for** i = 1 to ch **do**
2: **for** j = 1 to cw **do**
3: Generate a bit x, such that x = 1 with probability p and x = 0 with probability $1 - p$
4: **if** x == 1 **then**
$[AS_1(i,j), AS_2(i,j), ..., AS_n(i,j)]$ = generateSecretBits($WI(i,j), MS(i,j)$)
5: **else**
$[AS_1(i,j), AS_2(i,j), ..., AS_n(i,j)]$ = generateCoverBits($CI_1(i,j)$, $CI_2(i,j)$, ..., $CI_n(i,j)$)
6: **function** GENERATESECRETBITS(w, ms)
7: **if** $w == 0$ **then**
$m_1 = ms$
8: **else**
$m_1 = Complement(ms)$
9: **for** z in range(2, n) **do**
10: **if** $w == 0$ **then**
$m_z = m_{z-1}$
11: **else**
$m_z = Complement(m_{z-1})$
12: Return $[m_1, m_2, ...m_n]$
13: **function** GENERATECOVERBITS(c_1, c_2, ..., c_n)
14: **for** z **do** in range(1, n)
15: **if** $c_z == 0$ **then**
$m_z = 0\ or\ 1$
16: **else**
$m_z = 1$
17: Return $[m_1, m_2, ...m_n]$

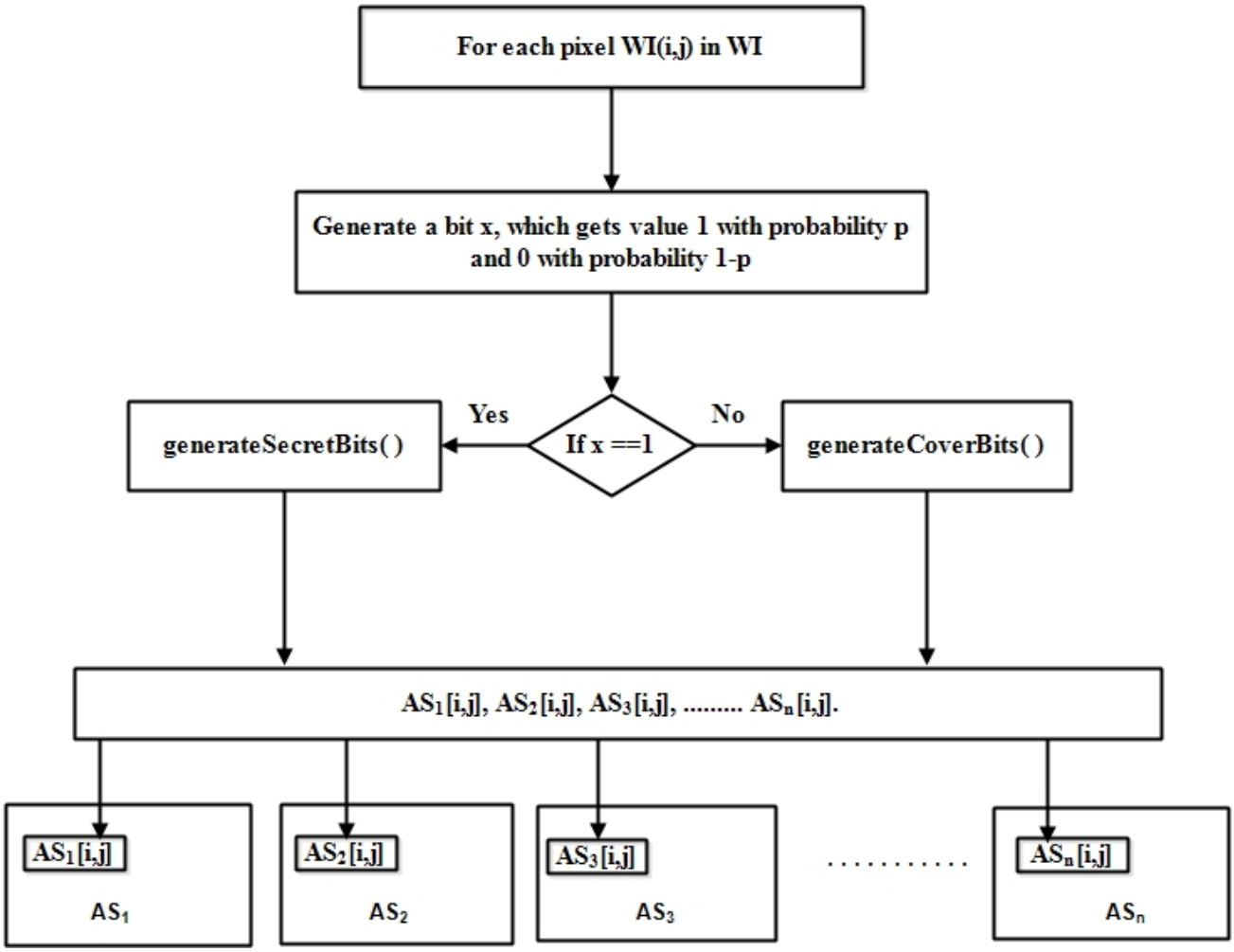


Figure 3.9: Generation of authentication Shares

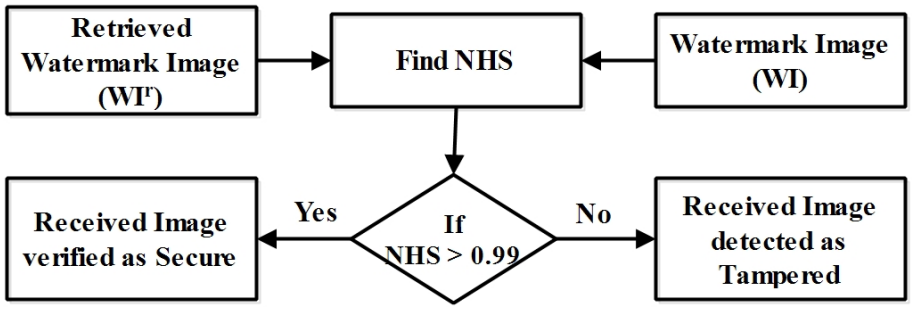
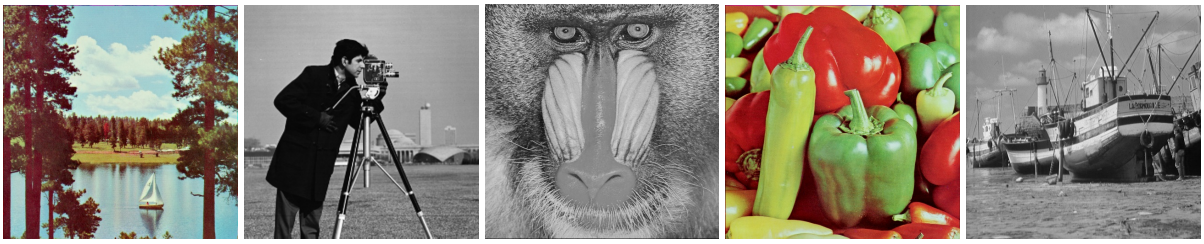


Figure 3.10: Tamper Detection Phase



(a) (b) (c) (d) (e)

Figure 3.11: Different input test images used in the proposed method (a) Lake (b) Cameraman (c) Baboon (d) Peppers (e) Boat

unity, then original and extracted watermarks are identical and host image is authentic otherwise it is tampered. This phase is shown in Figure 3.10.

An additional refinement process is applied to WI' to enhance the results of tamper detection. Logical *NOR* operation is applied between WI and WI' for the areas which have been detected as tampered while the rest of the pixels remain unmodified. This helps in enhancing the accuracy of tamper detection scheme.

3.4 Experimental Results and Discussion

The performance of the proposed scheme for digital images is implemented using MATLAB (R2018a), 64-bit (win64) software. The experiment is conducted on 8-bit host images and binary watermark image of size 512×512. The size of the watermark can be lesser than size of HI, but that would lead to pixel expansion while generating shares. Five test images *viz.* Lake, Cameraman, Baboon, Peppers, and Boat are used for experimentation purpose and presented in Figure 3.11.

To evaluate the effectiveness of the proposed authentication scheme, some standard measures *viz.* PSNR, SSIM and DR are used. Statistical Analysis of the scheme is also performed using parameters like *TPR*, *FPR* and accuracy. The efficiency of the proposed scheme is also tested against different tampering attacks. These measures and results are described in the following subsections.

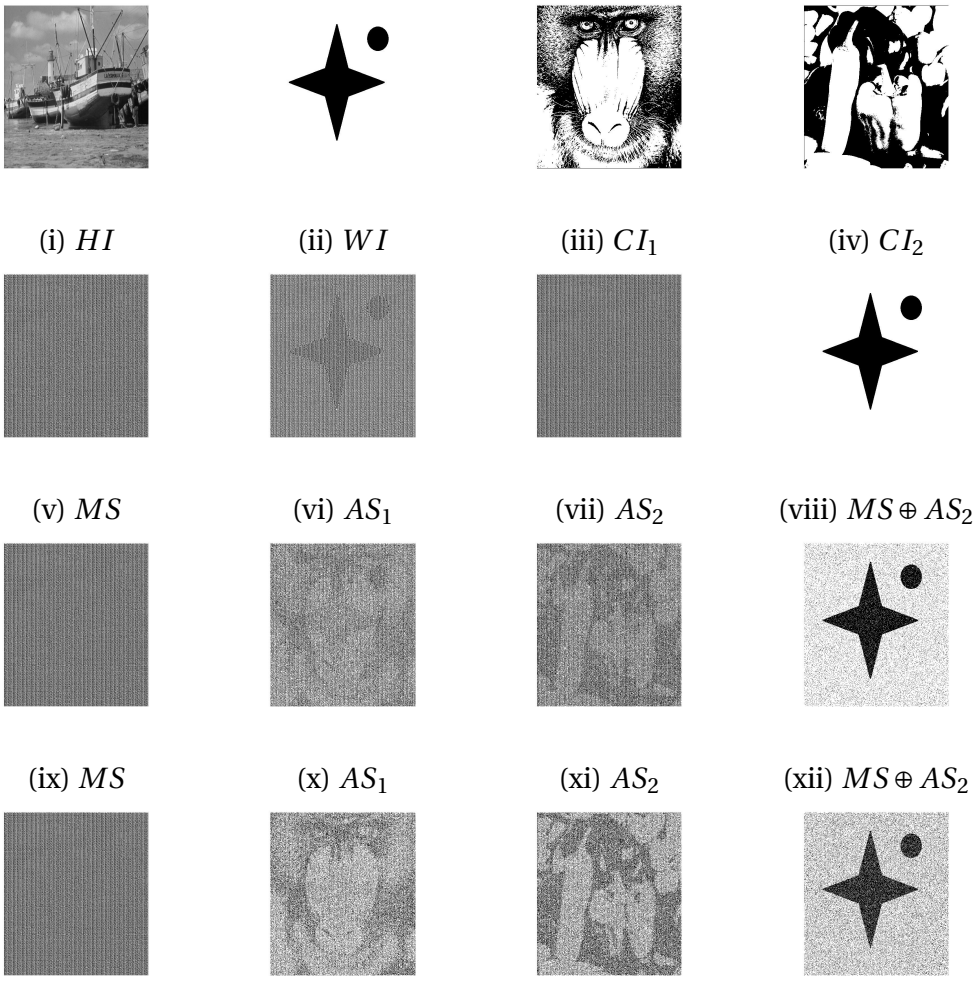
3.4.1 Quality Analysis

The parameters used to analyze the visual quality of generated authentication shares are PSNR and SSIM while NHS is used to analyze similarity between original WI and retrieved WI^r.

High value for PSNR shows better quality of the authentication share and least distorted. PSNR of authentication shares in the proposed scheme has been maintained above 50 *dB*, which is quite better with respect to the existing authentication schemes based on VC. This comparison has been shown in Table 3.3. PSNR of marked image with respect to original image tends toward infinity as watermark is not embedded into it. The SSIM values of the authentication shares generated has been shown in the Table 3.2 and it can be seen that the values are maintained close to 1.

Results for *(k = 2, n = 3)*-case of the scheme at successive values of p= 0, 0.2, 0.4, 0.6, 0.8, 1.0 have been shown in Table 3.1 (v)-(xviii). *(2,3)* represents that 3 shares are generated from the host image and atleast 2 shares are required to retrieve the watermark. The table shows *AS* and *MS* at different values of p.

Table 3.1: Simulation Results by Proposed Scheme for *(k = 2, n = 3)*



(xv) MS (xvi) AS_1 (xvii) AS_2 (xviii) $MS \oplus AS_2$

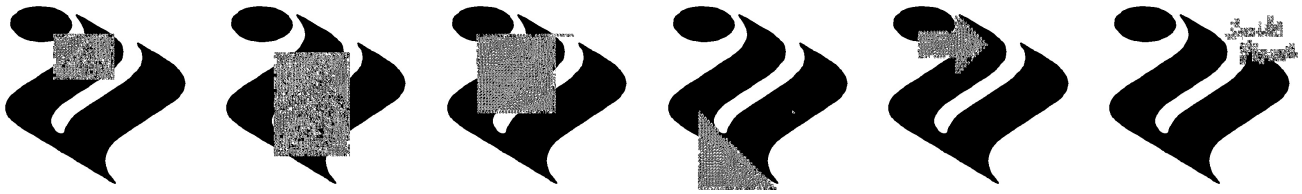
It can be observed from the Table 3.1 that as the value of p increases, the visual quality of authentication share images enhances while superimposed result image deteriorates. Thus, depending upon the application and the requirements, the value of p can be chosen,*i.e.* when the security of the shares being stored is the main concern, a larger value of p would be preferred while if the quality of the watermark retrieved is the main concern to verify the image authentication, smaller value of p can be chosen.

The performance of the proposed scheme is tested against five different tampering attacks on all test images. The tampered images and their detection results are shown in Figures 3.12-3.15.

It can be observed that the areas that were tampered in the original cameraman image shown in Figures 3.12 *(a-f)*, are visible as gray patches on the retrieved watermarks in Figures 3.12 *(g-l)*. Similarly, the tamper detection results for Boat, Peppers and Baboon against different tampered attacks, are shown in Figures 3.13 - 3.15.

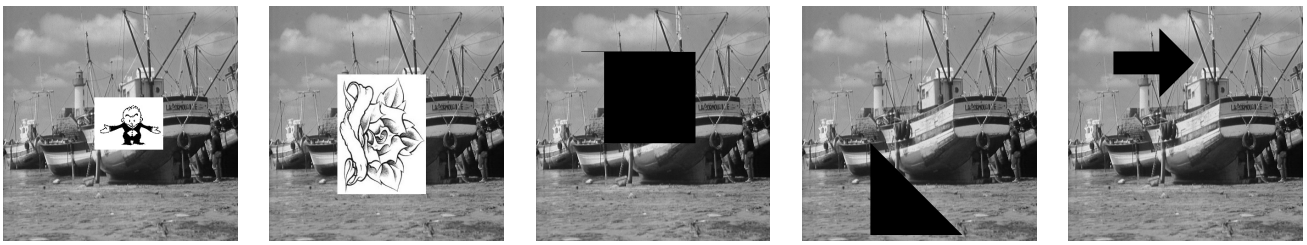
Thus, Figures 3.12-3.15 verify the effectiveness of the proposed scheme in terms of tamper detection. The areas tampered in the attacked images can be visually observed in the retrieved watermark as a gray colored patch.

(a) Attack 1 (b) Attack 2 (c) Attack 3 (d) Attack 4 (e) Attack 5 (f) Attack 6

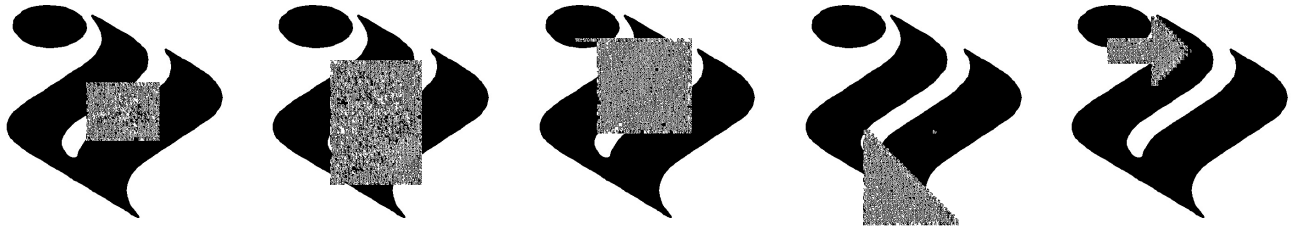


(g) Tamper Detection for Attack 1 (h) Tamper Detection for Attack 2 (i) Tamper Detection for Attack 3 (j) Tamper Detection for Attack 4 (k) Tamper Detection for Attack 5 (l) Tamper Detection for Attack 6

Figure 3.12: Different Tampering attacks and their Tamper Detection Results for Cameraman



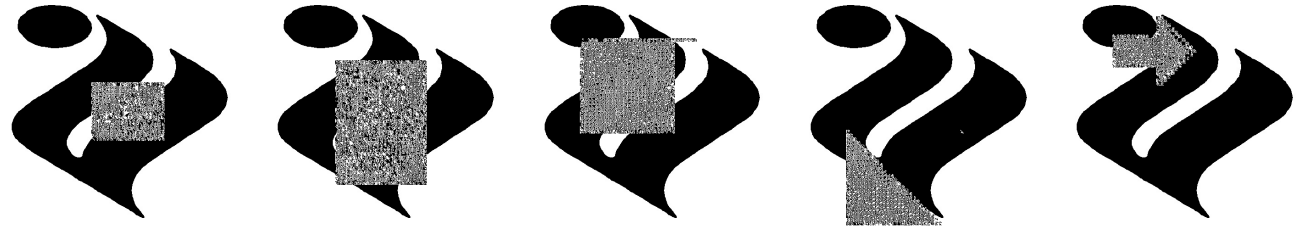
(a) Attack 1 (b) Attack 2 (c) Attack 3 (d) Attack 4 (e) Attack 5



(f) Tamper Detection for Attack 1 (g) Tamper Detection for Attack 2 (h) Tamper Detection for Attack 3 (i) Tamper Detection for Attack 4 (j) Tamper Detection for Attack 5

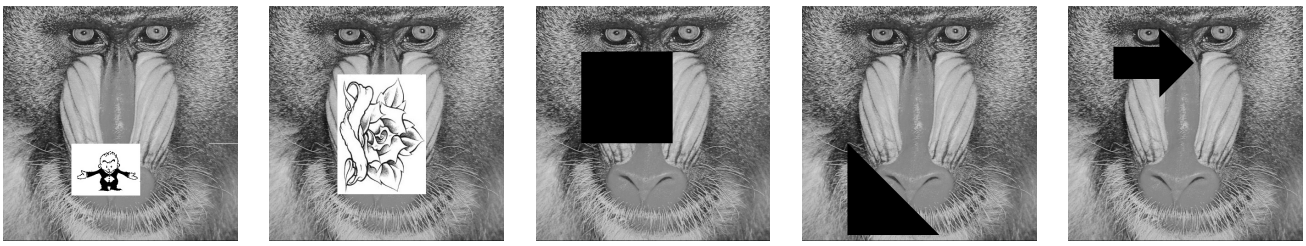
Figure 3.13: Different Tampering attacks and their Tamper Detection Results for Boat

(a) Attack 1 (b) Attack 2 (c) Attack 3 (d) Attack 4 (e) Attack 5

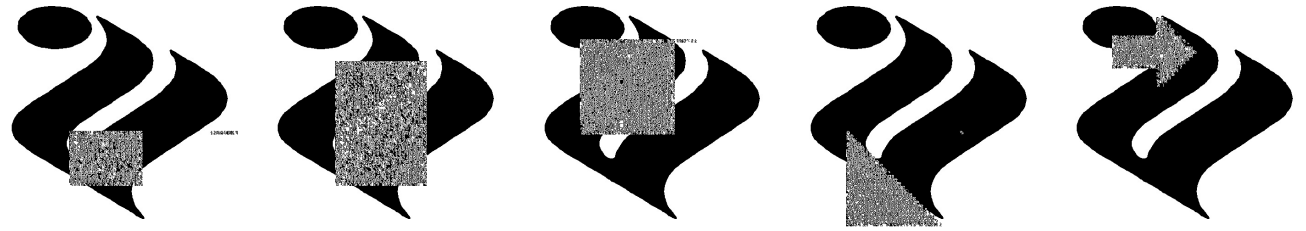


(f) Tamper Detection for Attack 1 (g) Tamper Detection for Attack 2 (h) Tamper Detection for Attack 3 (i) Tamper Detection for Attack 4 (j) Tamper Detection for Attack 5

Figure 3.14: Different Tampering attacks and their Tamper Detection Results for Peppers



(a) Attack 1 (b) Attack 2 (c) Attack 3 (d) Attack 4 (e) Attack 5



(f) Tamper Detection for Attack 1 (g) Tamper Detection for Attack 2 (h) Tamper Detection for Attack 3 (i) Tamper Detection for Attack 4 (j) Tamper Detection for Attack 5

Figure 3.15: Different Tampering attacks and their Tamper Detection Results for Baboon

Table 3.2: PSNR and SSIM of the authentication shares generated for different values of probability *(p)*

Probability *(p)*	PSNR		SSIM	
	AS_1	AS_2	AS_1	AS_2
0	54.92	54.29	0.9836	0.9806
0.25	53.04	53.26	0.9801	0.9772
0.5	52.12	52.42	0.9754	0.9741
0.75	51.53	51.74	0.97	0.97
1	51.14	51.16	0.965	0.964

Table 3.2 shows the PSNR and SSIM values for the authentication shares generated at different values of p. The results have been shown for AS_1 and AS_2 which are two authentication shares created using the cover images Baboon and Peppers, as shown in Figure 3.11.

It can be observed from the results that the PSNR of the generated authentication shares has been maintained above 50 *dB* and SSIM between the share images and the cover images has been maintained close to 1. The value of PSNR and SSIM decreases, as the value of p increases. Table 3.3 shows the comparison of the PSNR values of the authentication shares of the proposed scheme with the stego images of the existing schemes, that have been created to authenticate the host image. The results for the proposed scheme are shown for an average p value, *i.e.* $p = 0.5$.

It can be observed from the Table 3.3 that the PSNR of these images in the proposed scheme is maintained to be better as compared to the existing schemes. In the existing schemes, the stego images are created and stored with hash data and shares embedded into them. While, in the proposed scheme, instead of embedding any data, authentication shares are created using the MS, watermark and cover images.

The results of the proposed scheme for the statistical parameters are shown in Tables 3.5-3.9. Values in these tables show results obtained for various test images at different attacks. Referring to these tables, results clearly demonstrate that the algorithm shows high accuracy in tamper detection. It can be observed that for the blocks, accuracy is around 100% for most of the images at different attacks. For the pixels it is low as compared to blocks, but still it is quite high.

Table 3.3: Comparison with the existing schemes for the PSNR of the authentication shares generated

Schemes → Images ↓	Lin and Tsai (2004)	Chang et al. (2008)	Chang et al. (2011)	Eslami and Ahmadabadi (2011)	Yang et al. (2007)	Wu and Sun (2013b)	Ulutas et al. (2013)	Peng et al. (2018)	Proposed Scheme
Baboon	39.18	40.93	45.10	48.10	36.20	47.17	–	40.71	52.12
Lena	39.18	40.97	45.12	48.13	36.17	47.19	48.45	40.73	52.25
Pepper	39.16	40.96	45.1	48.12	36.18	47.18	–	40.72	52.42

Table 3.4: Statistical Analysis of tamper detection capacity in terms of pixels and blocks for Boat

Attack Index	T_{pixels}		X_{pixels}		TP		FP		TN		FN		TPR		FPR		Accuracy(%)	
	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks
1	262144	4096	17097	300	10595	299	6502	1	245047	3796	989	0	0.9146	1	0.0258	0.0002	97.52	99.98
2	262144	4096	50321	849	32397	848	17924	1	211823	3247	1907	0	0.9444	1	0.0780	0.0003	93.16	99.98
3	262144	4096	40000	682	26763	680	13237	2	222144	3414	1738	0	0.9390	1	0.0562	0.0005	94.95	99.95
4	262144	4096	20100	377	15700	377	4400	0	242044	3719	1931	0	0.8905	1	0.0179	0	98.32	100
5	262144	4096	10700	203	8025	203	2675	0	251444	3893	1136	0	0.8760	1	0.0105	0	98.98	100

Table 3.5: Statistical Analysis of tamper detection capacity in terms of pixels and blocks for Baboon

Attack Index	T_{pixels}		X_{pixels}		TP		FP		TN		FN		TPR		FPR		Accuracy(%)	
	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks
1	262144	4096	17012	308	10010	308	7002	0	245132	3788	1308	0	0.8844	1	0.0278	0	97.33	100
2	262144	4096	50332	850	32898	850	17434	0	211812	3246	2016	0	0.9423	1	0.0760	0	93.35	100
3	262144	4096	40000	682	26546	682	13454	0	222144	3414	1732	0	0.9388	1	0.0571	0	94.87	100
4	262144	4096	20100	352	17319	352	2781	0	242044	3414	1185	0	0.9360	1	0.0114	0	98.94	100
5	262144	4096	12700	227	9579	227	3121	0	249444	3869	790	0	0.9238	1	0.0124	0	98.81	100

Table 3.6: Statistical Analysis of tamper detection capacity in terms of pixels and blocks for Cameraman

Attack Index	T_{pixels}		X_{pixels}		TP		FP		TN		FN		TPR		FPR		Accuracy(%)	
	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks
1	262144	4096	17088	300	10515	295	6573	5	245056	3796	991	0	0.9139	1	0.0269	0.0013	97.49	99.88
2	262144	4096	50329	849	31788	841	18541	8	211815	3247	1943	0	0.9424	1	0.0805	0.0025	92.93	99.80
3	262144	4096	39970	682	26549	680	13421	2	222174	3414	1543	0	0.9451	1	0.0570	0.0005	94.88	99.95
4	262144	4096	20092	352	17289	350	2803	2	242052	3744	1027	0	0.9439	1	0.0114	0.0005	98.93	99.95
5	262144	4096	12697	227	9748	223	2949	4	249447	3869	712	0	0.9319	1	0.0117	0.0010	98.88	99.90

Table 3.7: Statistical Analysis of tamper detection capacity in terms of pixels and blocks for Peppers

Attack Index	T_{pixels}		X_{pixels}		TP		FP		TN		FN		TPR		FPR		Accuracy(%)	
	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks
1	262144	4096	17099	319	11556	319	5543	1	245045	3777	1575	0	0.8801	1	0.0221	0	97.89	100
2	262144	4096	50313	849	32226	848	18087	1	211831	3247	1921	0	0.9437	1	0.0787	0.0003	93.10	99.98
3	262144	4096	40000	680	26464	680	13536	2	222144	3414	1639	0	0.9417	1	0.0574	0.0005	94.84	99.95
4	262144	4096	20100	352	17300	350	2800	2	242044	3744	1238	0	0.9332	1	0.0114	0.0005	98.93	99.95
5	262144	4096	12700	224	9746	224	2954	3	249444	3869	838	0	0.9208	1	0.0117	0.0007	98.87	99.93

Table 3.8: Statistical Analysis of tamper detection capacity in terms of pixels and blocks for Lake

Attack Index	T_{pixels}		X_{pixels}		TP		FP		TN		FN		TPR		FPR		Accuracy(%)	
	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks
1	262144	4096	17097	300	9992	299	7105	1	245047	3796	1028	0	0.9067	1	0.0282	0.0002	97.29	99.98
2	262144	4096	50304	849	32453	848	17851	1	211840	3247	1919	0	0.9442	1	0.0777	0.0003	93.19	99.98
3	262144	4096	40000	682	26517	682	13483	0	222144	3414	1657	0	0.9412	1	0.0572	0	94.86	100
4	262144	4096	20100	352	17270	352	2830	0	242044	3744	1115	0	0.9394	1	0.0116	0	98.92	100
5	262144	4096	12700	227	9571	227	3129	0	249444	3869	877	0	0.9161	1	0.0124	0	98.81	100

Table 3.9: Timing Analysis for Different Images (in seconds)

Images → Algorithms ↓	Boat	Baboon	Lena	Lake	Peppers	Cameraman
MS Construction	29.82	36.77	31.84	34.50	30.61	31.80
Authentication Shares Construction	0.64	0.65	0.59	0.61	0.59	0.83
Authentication Phase	46.25	49.55	43.52	46.28	43.72	46.05

Table 3.9 shows the timing analysis of the scheme for different images. Table 3.10 shows the tampered detection rate of both cases for different images and at different attacks. It can be observed that the proposed scheme shows very high tampered detection rate for Case B while its satisfactory for Case A.

Table 3.11 shows the comparison of the proposed scheme with existing image authentication schemes. In the table, the first column shows different authentication schemes. Subsequently, performance evaluation matrices such as PSNR, the similarity between extracted and embedded watermark and tamper detection ability are compared. It can be observed that as the scheme uses VC, the watermark is not embedded inside the host image, but is hidden in the shares generated. Hence PSNR of the marked image with respect to original image tends toward infinity. Also, as XOR operation is used to superimpose MS and AS, which ensures maximum similarity between the original and extracted watermark, NHS tends towards 1. Methods suggested by other authors embed the watermark into the host image, hence the PSNR value decreases. Tamper detection ability of the proposed scheme is also high which has been shown in the results. The '-' in the table shows the corresponding data is not available in respective papers.

Table 3.12 provides a comparison of the proposed scheme with existing VC-based image authentication schemes. The proposed scheme uses CA to create shares using the host image and watermark. Thus, unlike the existing schemes, there is no need to insert watermarks within the host image. At the receiver's side, this watermark can be extracted simply by superimposing the shares without the use of a sophisticated extraction algorithm. This reduces the complexity of the scheme. As the mean of every block is used as a key, there is no need to transmit any side information, as the mean can be determined by the sender and the recipient independently.

Table 3.10: Detection Rate for Different Images at Different Attacks

Images	Boat		Baboon		Lena		Lake		Peppers		Cameraman	
Attack Index	Case A	Case B	Case A	Case B	Case A	Case B	Case A	Case B	Case A	Case B	Case A	Case B
1	66.91	99.67	58.84	100	67.48	100	58.44	99.67	67.58	100	61.53	98.33
2	64.38	99.88	65.36	100	64.57	99.41	64.51	99.88	64.05	99.88	63.16	93.06
3	66.91	99.71	66.36	100	61.25	100	66.29	100	66.16	99.71	66.42	99.71
4	78.10	100	86.16	100	85.93	100	85.92	100	86.07	99.43	86.05	99.43
5	75.00	100	75.43	100	75.55	100	75.36	100	76.74	98.68	76.77	98.24

Table 3.11: Comparison of proposed scheme with recent image authentication schemes

Technique	Scheme	PSNR*(dB)*	Similarity factor	Tamper Detection/Localizing	Embedding Required
Chuang and Hu (2011)	VQ Scheme	≈ 34	-	Possible	Yes
Shen and Chen (2012)	DWT based scheme	≈ 30	NC=0.98	Not discussed	Yes
Preda (2013)	DWT based scheme	≈ 40	-	Possible	Yes
Al-Otum (2014)	DWT quantization	≈ 41	-	Possible, can detect 8 × 8 region	Yes
Li et al. (2015)	Two Level DWT	≈ 36	NC=0.8	Possible,localization accuracy medium	Yes
Li et al. (2016)	Vector Quantization Scheme	≈ 31.3	SSIM = 0.88	Possible	Yes
Shojanazeri et al. (2017)	DWT and Zernike moments	≈ 40.9	-	Possible	Yes
Singh and Singh (2017a)	DCT based scheme	≈ 39.3	NC = 0.98	Possible	Yes
Tiwari et al. (2017)	Two stage VQ technique	≈ 42	NHS = 1.0	Possible	Yes
Proposed Work	VC based scheme	*Infinite*	NHS ≈ 1.0, NC = 1.0	Possible, accuracy is very high	No

Table 3.12: Comparison of proposed scheme with existing image authentication schemes based on VC

Scheme	Share Creation	Authentication Data	Embedding Required	Extraction Scheme	Pixel Expansion	Storage Cost for Shares	Transmission Cost for Side Information	Accuracy %
Lin and Tsai (2004)	Polynomial based VC	Parity bits	Yes	Extraction and Overlapping	-	Yes	Yes	-
Chang et al. (2008)	Polynomial based VC	Chinese Remainder Theorem	Yes	Extraction and Overlapping	-	Yes	Yes	-
Eslami and Ahmadabadi (2011)	Polynomial based VC	Hash Function	Yes	Extraction and Overlapping	-	Yes	Yes	-
Wu and Sun (2013b)	Cellular Automata	Hash Function	Yes	Extraction and Overlapping	-	Yes	Yes	-
Ulutas et al. (2013)	Polynomial based VC	Hash Function	Yes	Extraction and Overlapping	-	Yes	Yes	-
Srividhya et al. (2016)	Traditional VC	Authentication Image	No	Extraction and Overlapping	-	Yes	Yes	-
Proposed Work	Cellular Automata and Traditional VC	Watermark	No	XOR- Overlapping	No	Partial	No	High

This saves the expense of transmission. In the existing schemes, all the shares created must be stored with recipients which are later superimposed together to recover the watermark, whereas only one share must be stored in the proposed scheme, as the other share is self-generated using CA. All algorithms can find tamper detection, but accuracy is either limited or not calculated. Most of the schemes reported did not indicate any way of quantitatively classifying attacks. While in the proposed scheme, a complete statistical study of the system has been carried out and shown for different images and attacks, demonstrating high accuracy.

3.4.2 Security Analysis

To prove the security of the proposed scheme, it has been analyzed using the following security aspects:

Construction of Shares

Unlike the existing authentication schemes(Preda (2013); Shojanazeri et al. (2017); Li et al. (2015); Al-Otum (2014); Singh and Singh (2017a); Li et al. (2016); Chuang and Hu (2011)) based on watermarking, the watermark is not embedded inside the host image, but it is used to construct shares. This makes it very difficult to detect or recover the watermark from marked image, thereby making the scheme more secure.

Meaningful Shares

The meaningless random-looking shares created in the conventional VC schemes usually eventually lead to the suspicion that some secret information is being exchanged which is a security threat. Meaningful authentication shares have therefore been created in the proposed scheme to ensure the security in the proposed scheme.

k out of *n* scheme

The watermark image has been used to ensure the authentication of the shares generated, thereby enhancing the security. The watermark can be revealed only when k participants superimpose their shares including MS generated from host image. No less than k shares have the ability to extract the watermark. This ensures the security of the scheme.

3.4.3 Time Complexity

The primary time-consuming operations of the proposed scheme are: WPD, *CA*, MS Construction and OS Construction. As WPD takes $O(n\log n)$, *CA* takes $O(n)$ time, thus, total time complexity for Algorithm 3.1 is accounted to $O((\frac{n}{bh\times bw}) \times (nlog\ n+n)$ where n denotes the size of host image. The time-costing of MS and OS Construction and their superimposition usually involve binary operations on all pixels, hence their complexity can be accounted to $O(n)$. Thus, the time complexity of the scheme is $O(n^2\log n)$.

3.5 Conclusion of the Chapter

In this Chapter, an authentication scheme based on *WPD*, *VC* and *CA* is proposed. The tampered areas are detected just by XOR-superimposition of shares, thus reducing computational complexity. Experimental results and discussions demonstrate the efficiency of the proposed scheme in terms of imperceptibility, extraction of the hidden watermark with minimum complexity, high accuracy in tamper detection, high security due to meaningful shares, low storage cost and low transmission cost. Also, as compared to some reported authentication schemes based on VC, the proposed scheme can directly generate meaningful authentication shares with watermark, host and cover image information, without any extra data hiding process. Tamper detection rate and accuracy have been observed more than 99% for different images against different tamper attacks. The proposed scheme can be extended to color images.

CHAPTER 4

Curvelet Transform based Robust Copyright Protection Scheme for Color Images using Baker Map

.

4.1 Introduction

A robust copyright protection scheme using *DCuT* and *EVCS* is proposed for color images which creates non expanded noiseless shares. MS is created using low and middle frequency *DCuT* coefficients. OS is created using MS and the watermark with the reference of the codebook. When MS and OS are superimposed using XOR operation, the watermark is retrieved that is used to verify the copyright. Security of the scheme is assured by creating meaningful OS; and by using Baker Map for scrambling watermark and transformed host image. The scheme is proved to be imperceptible

Contents of the work presented in this Chapter have been conditionally accepted in *Computers and Electrical Engineering*. (SCI Indexed)

and robust against several image processing attacks. The scheme is compared with some existing copyright protection schemes to prove its effectiveness.

4.2 Preliminaries

This section discusses DCuT and Baker Map that are used in the proposed scheme.

4.2.1 Discrete Curvelet Transform

DCuT which is a multiresolution transform was proposed by Candès and Donoho (2004). It imparts a sparser representation of images as compared to other transforms. To represent an image, *FrFT* and *DWT* need a higher number of frequency coefficients and wavelet basis functions, respectively. *DCuT* represents edges and curves information of the image. For an image $I(x, y)$, *DCuT* generates coefficients using:

$$C^D(sc, ot, tr) = \sum_{0 \le x, y \le h} f(x, y)^{\theta^D_{sc,ot,tr}(x,y)} \quad \ldots (4.1)$$

Here, $\theta^D_{sc,ot,tr}(x, y)$ represents digital curvelet waveform of a cartesian array of form $f(x, y)$ where $0 \le x, y \le h$. $h \times h$ represents image size. *sc*, *ot* and *tr* refer to scale, orientation and translation parameters, respectively. According to Candès and Donoho (2004), there are two variations of *DCuT*: Unequi-spaced Fast Fourier Transform (FFT) and Frequency Wrapping (WRAP). Image watermarking and compression applications mostly use WRAP due to it's simpler implementation and low computation time as compared to Unequi-spaced FFT. WRAP based DCuT is graphically represented in Figure 4.1. WRAP is implemented as follows:

(i) Obtain Fourier samples $\hat{f}[i_1, i_2]$ by applying 2D FFT on image.

(ii) For every scale *sc* and angle *ot*

  (a) Perform: $\hat{f}[i_1, i_2] \times \hat{u}_{j,l}[i_1, i_2]$

  (b) Wrap this result around origin

  (c) Obtain discrete coefficients by applying inverse 2D FFT to the wrapped data.

The obtained curvelet coefficients $C(sc, ot, tr)$, where sc, ot and tr represent scale, direction and translation parameters, respectively, are divided into three frequency sub-bands: Low Fre-

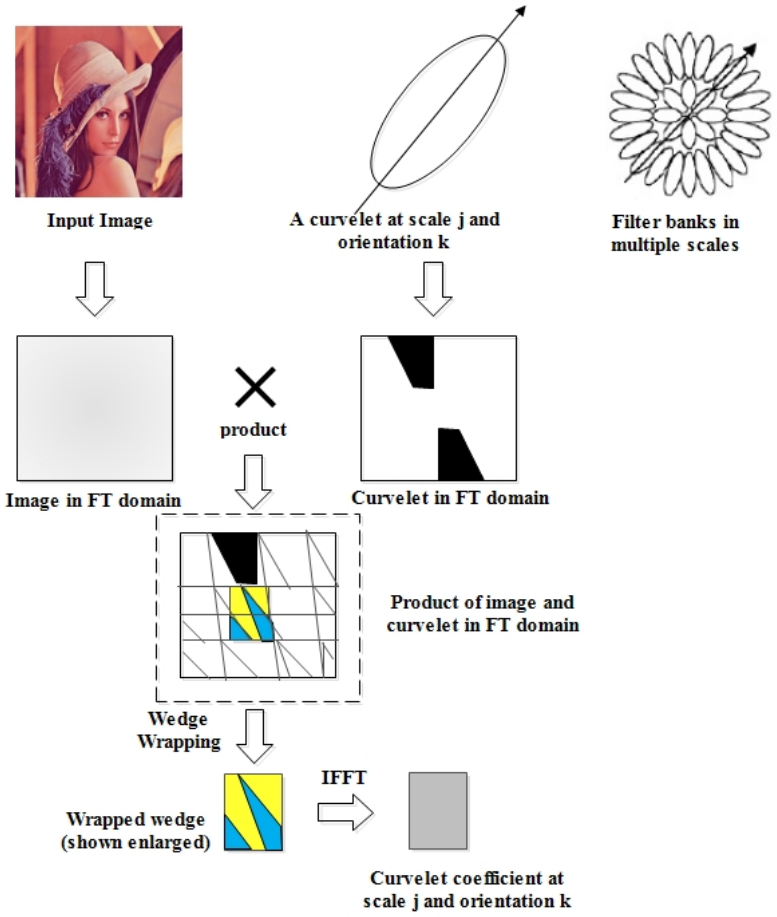
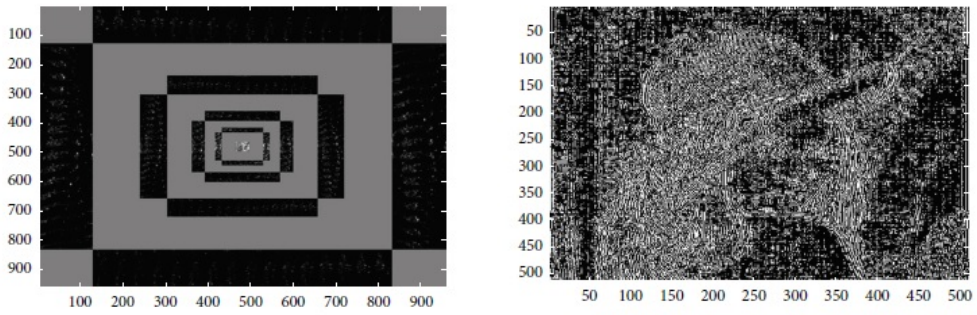


Figure 4.1: Frequency wrapping based DCuT



(a) (b)

Figure 4.2: The coefficient matrix image of (a) first five layers (b) sixth layer via Curvelet transform for Lena

quency *(LF)*, Middle Frequency *(MF)* and High Frequency *(HF)*. The coefficient count in every subband depends on the image size. For example, an image of size 512×512 is decomposed using *DCuT-WRAP* into different cells, represented as C(1,1), C(1,2), C(1,3), C(1,4), C(1,5), C(1,6), with 6 scale parameters and 16 orientation parameters. The innermost cell C(1,1) consists *LF* coefficients, middle cells C(1,2) to C(1,5) contain *MF* coefficients and the outermost C(1,6) contains *HF* coefficients and is equal to the image size. *LF* and *MF* coefficients provide better robustness to the scheme as compared to *HF*. The watermark is retrieved successfully to prove the copyright, even when the image is attacked by different image processing attacks. Coefficient matrix images of the inner five layers and outermost layer for Lena image constructed using *DCuT* is shown in Figure 4.2.

4.2.2 Baker Map

In Baker map (Fox (1997)), the pixel positions of the image are shuffled and then this matrix is bijected onto itself, to scramble the image without affecting the pixel values. The bijection can be performed in two ways (Driebe (1999)), either the upper section remains unfolded or one of the sliced halves is folded onto other. These scenarios have been represented mathematically in (4.2), as follows:

$$I(x,y) = \begin{cases} [x_{i+1}, y_{i+1}] = [2x_i, \frac{y_i}{2}], & \text{for } 0 \le x_i < \frac{1}{2} \\ [x_{i+1}, y_{i+1}] = [2(1-x_i), 1-\frac{y_i}{2}], & \text{for } \frac{1}{2} \le x_i < 1 \end{cases} \quad \ldots (4.2)$$

where x_0 and y_0 are initialized with some random values .

$$BM(x,y) = \begin{cases} 0, & \text{for } 0 \le x_i < \frac{1}{2} \\ 1, & \text{for } \frac{1}{2} \le x_i < 1 \end{cases} \quad \ldots (4.3)$$

To scramble the image, XOR operation is applied between Baker binary matrix instance obtained through (4.3) and the corresponding bit in the unscrambled image. To unscramble the image, these steps are applied in reverse order.

Agarwal (2018) has analyzed various scrambling techniques and it shows that Baker Map outperforms Arnold and Henon Map Transform. PSNR of image scrambled by Baker Map is less than the images transformed by Arnold and Henon Map Transforms. Also, Baker Map is faster as compared to the other scrambling transforms.

4.2.3 K-means Clustering

K-means (MacQueen (1967)) is a simple unsupervised learning technique to create the clustering. Given a dataset, this technique decides K centroids such that they should have maximum distance possible between them. Every point in dataset is randomly associated with the nearest centroid. This procedure is repeated in loop, resulting into optimal centroids and bindings. It can be noticed that K centroids change their location after every loop, until no more changes occur. Thus, the technique aims at minimizing the following objective function:

$$J = \sum_{j=1}^{k} \sum_{i=1}^{n} \left\| x_i^j - c_j \right\|^2 \quad \ldots (4.4)$$

where $\left\| x_i^j - c_j \right\|^2$ refers to distance between chosen data point x_i^j and the cluster centroid c_j.

4.3 Proposed Scheme

The proposed scheme is divided into two phases: Share Construction and Copyright Verification. Implementation of these two phases are shown in Figures 4.3 and 4.4.

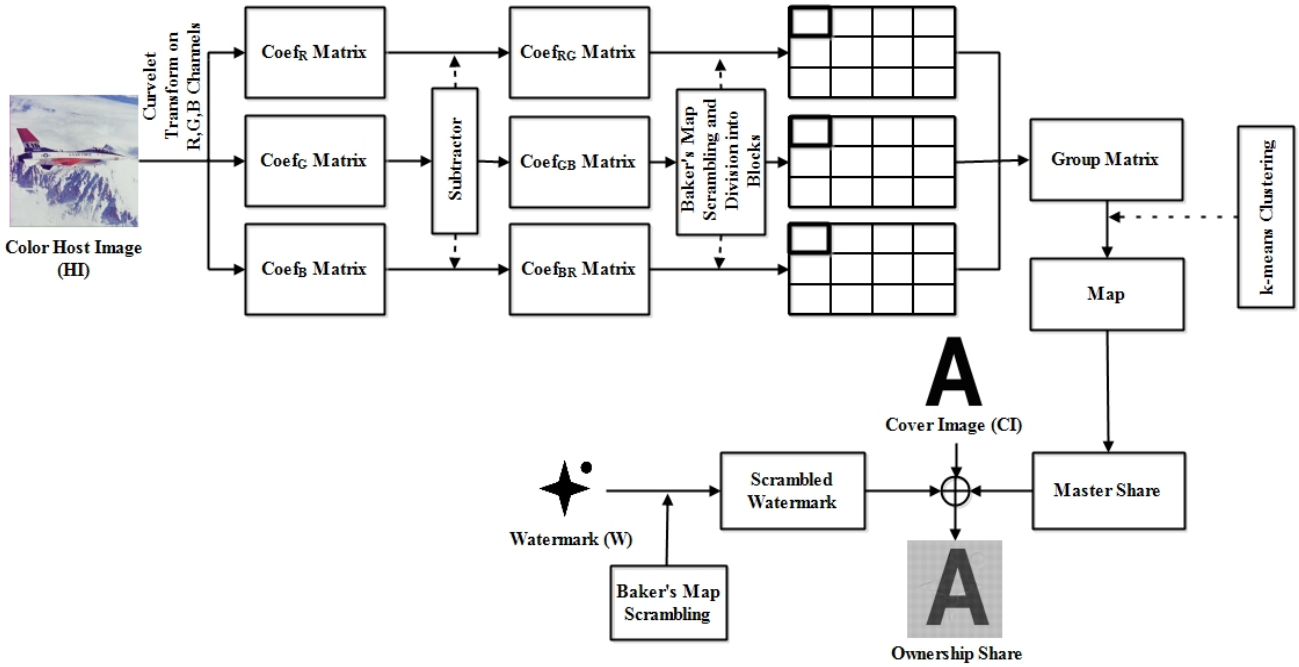


Figure 4.3: Block Diagram for Share Construction Phase

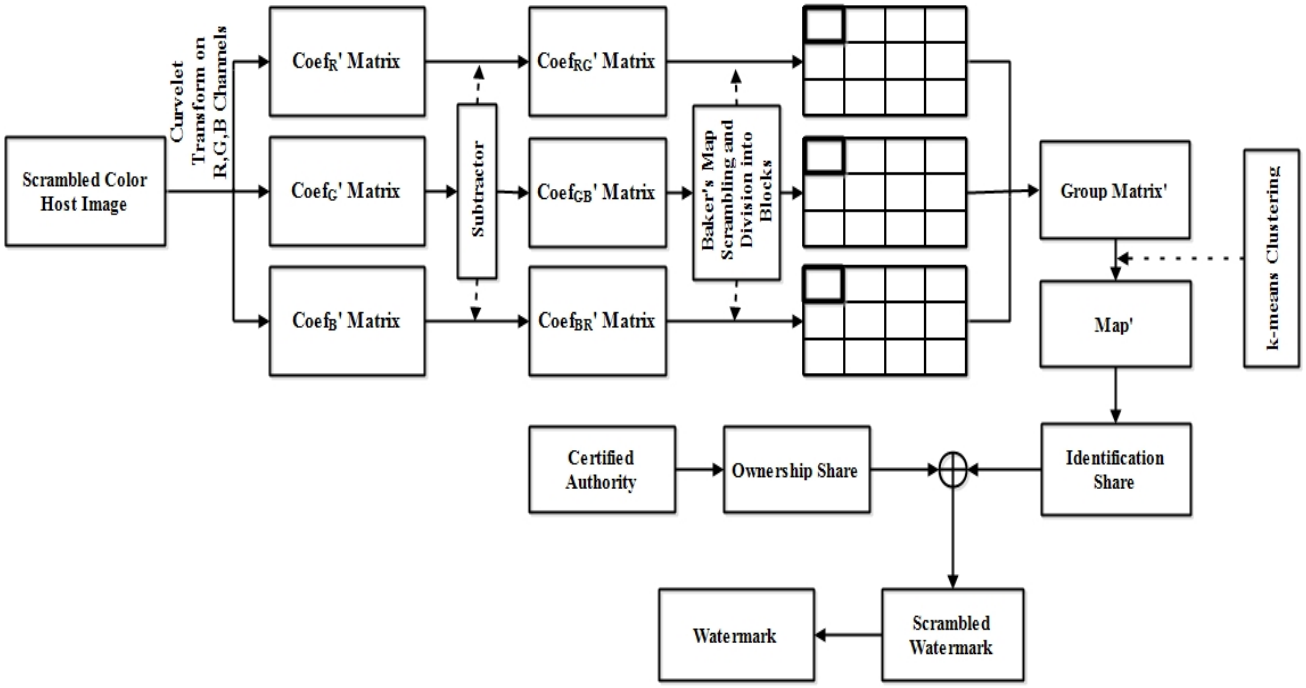


Figure 4.4: Block Diagram for Copyright Verification Phase

4.3.1 Share Construction

In this phase, *MS* is constructed using *R*, *G* and *B* channels of the color image. *DCuT*-Wrapping is applied individually on every image channel. *LF* and *MF* sub-bands are used instead of *HF*, to construct the coefficient matrix for every channel. Human eyes are more sensitive to *LF* than *HF* information, thus choosing the inner layers help in enhancing robustness of the scheme. Inter layer subtraction is performed on the constructed coefficient matrices so that every transformed component now contains information about two layers and helps in improving robustness. These matrices are then concatenated to form a single matrix. Baker map is applied to the obtained coefficient matrix and watermark, to enhance security.

First *MS* is constructed using *K*-means clustering on the obtained coefficient matrix. Then, *MS*, *WI* and *CI* are together used to construct a noiseless *OS* using a codebook that has been prepared based on the following criteria:

i. The *OS* block pixels should bear a resemblance to the corresponding *CI* bit, *i.e.* if $CI_{bit} == 0$, then count of 0s > count of 1s in corresponding *OS* block and if $CI_{bit} == 1$, count of 1s > count of 0s in corresponding *OS* block.

ii. When corresponding *OS* and *MS* block bits are XOR-superimposed, *W* block is retrieved. This block is reduced to the watermark bit using equation 4.10. This signifies that if $W_{bit} == 0$, the

corresponding *OS* and *MS* block pixels should be as similar as possible to each other and if $W_{bit} == 1$, they should be as different as possible.

Four matrices of the form $M_{c,d}$ have been represented below, where c and d represent bit values of *WI* and *CI*, which are in set $\{0,1\}$.

$$M_{00} = \begin{bmatrix} 0&0&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \\ 0&0&1&0 \\ 0&1&0&0 \\ 0&1&0&0 \\ 0&1&0&0 \\ 0&1&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \end{bmatrix}, \quad M_{01} = \begin{bmatrix} 0&1&1&1 \\ 0&1&1&1 \\ 0&1&1&1 \\ 0&1&1&1 \\ 0&1&1&1 \\ 0&1&1&1 \\ 0&1&1&1 \\ 0&1&1&1 \\ 1&1&1&0 \\ 1&1&0&1 \\ 1&1&1&0 \\ 1&0&1&1 \\ 1&1&1&0 \\ 1&1&0&1 \\ 1&1&1&0 \\ 1&1&1&1 \end{bmatrix}, \quad M_{10} = \begin{bmatrix} 0&0&0&1 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 0&0&0&1 \\ 0&0&0&1 \\ 0&0&0&1 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \\ 0&0&0&1 \\ 0&0&0&1 \end{bmatrix}, \quad M_{11} = \begin{bmatrix} 1&1&1&0 \\ 1&1&1&0 \\ 1&1&0&1 \\ 1&1&1&0 \\ 1&0&1&1 \\ 1&0&1&1 \\ 1&0&1&1 \\ 1&1&1&0 \\ 0&1&1&1 \\ 0&1&1&1 \\ 0&1&1&1 \\ 0&1&1&1 \\ 0&1&1&1 \\ 0&1&1&1 \\ 0&1&1&1 \\ 0&1&1&1 \end{bmatrix} \quad \ldots (4.5)$$

After *OS* is constructed, *WI* is secretly stored with the copyright owner while *OS* is registered with a *TA* that can be used in the copyright verification, when required.

The share construction steps are described in Algorithm 4.1. Construction of *OS* block from *MS* and *W* blocks has been demonstrated with the help of an example in Figure 4.5(a). In Figure 4.5(a), blocks of size 2×2 are chosen from *CI* and *W*. The *Map* shown is created from HI following the steps described in Algorithm 4.1. Two random rows, $x = 1$ and $y = 14$ are selected from *M* that further represents 0 and 1, respectively. Thus, MS is constructed by replacing 0 and 1 in *Map* with patterns "0001" and "1110", respectively. As the first bit in *Map* is 0, the x^{th} row is chosen from $M_{c=0,d=1}$ and positioned in corresponding *OS* block, where c and d represent corresponding bits in *WI* and *CI* respectively.

Algorithm 4.1 Share Construction Phase

Input: HI of size $hh \times hw$, WI of size $wh \times ww$, CI of size $ch \times cw$
Output: MS and OS

1: Apply Curvelet decomposition on *R,G,* and *B* channels to get their coefficient matrices. Extract the LF and MF sub-bands from these matrices and combine theme to store as $Coef_R, Coef_G, Coef_B$, respectively for every channel. These sub-bands are further processed through subtractors to obtained inter-layer transformed component matrices ($Coef_{RG}, Coef_{GB}, Coef_{BR}$), described in equations 4.6 to 4.8.

$$Coef_{RG} = Coef_R - Coef_G \quad \ldots(4.6)$$

$$Coef_{GB} = Coef_G - Coef_B \quad \ldots(4.7)$$

$$Coef_{BR} = Coef_B - Coef_R \quad \ldots(4.8)$$

2: Scramble $Coef_{RG}$, $Coef_{GB}$, $Coef_{BR}$ and WI using Baker Map.
3: Segment the coefficient matrices into blocks b_i of size $bh \times bw$, where i = 1 to nb, $nb = \lceil \frac{hh \times hw}{bh \times bw} \rceil$. The matrices of blocks are represented as $rblock_i$, $gblock_i$, $bblock_i$
4: **for** i= 1 to nb **do**
Concatenate the corresponding blocks of three matrices into a single matrix C_i
5: Classify the blocks in C_i into 2 clusters: Cluster 0 and 1, using k-means clustering and store them as *Map* that contains cluster number for every corresponding block.
6: Construct MS corresponding to *Map* using M given in (4.9). Choose 2 different rows from the M for *Map* values '0' and '1'. Let the decimal value of the chosen row for '0' and '1' are represented by x and y respectively. Replace '0' and '1' in the *Map* with the chosen x^{th} and y^{th} rows, respectively to construct MS.

$$M = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad \ldots(4.9)$$

7: Construct *OS* using *Map, WI* and *CI* by following (4.5). This procedure has been explained as follows:
8: **for** i: 1 to mw **do**
9: **for** j: 1 to mh **do**
10: **if** *Map*(i,j)==0 **then**
Choose x^{th} row from $M_{c,d}$ and place it at the corresponding position in *OS*.
11: **else**
Choose y^{th} row from $M_{c,d}$ and place it at the corresponding position in *OS*.

4.3.2 Copyright Verification

During copyright verification phase, an Identfication Share (*IS*) is constructed from the received *HI* by following the MS construction steps described in previous section. The registered *OS* with *TA* is retrieved and superimposed with *IS* to obtain an expanded watermark. To prove the copyright, this watermark is resized to its original size and compared with the original watermark stored with owner. These steps are described in Algorithm 4.2 with an example demonstrated in Figure 4.5-(b) that shows the superimposition of *IS* and *OS* blocks to retrieve the watermark block.

Algorithm 4.2 Copyright Verification

Input: Received Host Image (HI') of size $hh \times hw$
Output: *IS*

1: Apply Curvelet decomposition on *R,G,* and *B* channels to get their coefficient matrices. Extract the LF and MF sub-bands from these matrices and combine theme to store as $Coef_R, Coef_G, Coef_B$, respectively for every channel. These sub-bands are further processed through subtractors to obtained inter-layer transformed component matrices ($Coef_{RG}, Coef_{GB}, Coef_{BR}$), described in equations 4.6 to 4.8.
2: Scramble $Coef_{RG}$, $Coef_{GB}$, $Coef_{BR}$ and WI using Baker Map.
3: Segment the coefficient matrices into blocks b_i of size $bh \times bw$, where i = 1 to nb, $nb = \lceil \frac{hh \times hw}{bh \times bw} \rceil$. The matrices of blocks are represented as $rblock'_i$, $gblock'_i$, $bblock'_i$
4: **for** i= 1 to nb **do**
Concatenate the corresponding blocks of three matrices into a single matrix C_i
5: Classify the blocks in C_i into 2 clusters: Cluster 0 and 1, using k-means clustering and store them as *Map'* that contains cluster number for every corresponding block.
6: Construct *IS* corresponding to *Map'* using the M given in (4.9). Choose the same 2 rows from M for *Map* values '0' and '1', that were chosen during the Share Construction Phase. Let the decimal value of the chosen row for '0' and '1' are represented by x and y respectively. Replace '0' and '1' in the *Map* with the chosen x^{th} and y^{th} row, respectively to construct *IS*.
7: Retrieve *OS* from *CA*.
8: Retrieve Watermark Image W' by stacking *OS* and *IS* using *XOR* operation.
9: Perform reduction process to obtain reduced RW' of size $wh \times ww$ by following rules:

$$w = \begin{cases} 1, & if \ \sum_j \sum_k s'_{j,k} \geq 2 \\ 0, & if \ \sum_j \sum_k s'_{j,k} < 2 \end{cases} \quad \ldots (4.10)$$

where w is a binary pixel in RW', $s'_{j,k}$ represent pixels in *W'* blocks of size 2×2.
10: Scramble the Watermark *W'* to obtain descrambled watermark *W"*.

4.4 Experimental Results and Analysis

A series of experiments are performed using MATLAB (R2018a), 64-bit (win64) software, on different color images of size 512×512 and binary watermark image of size 256×256, to analyze the

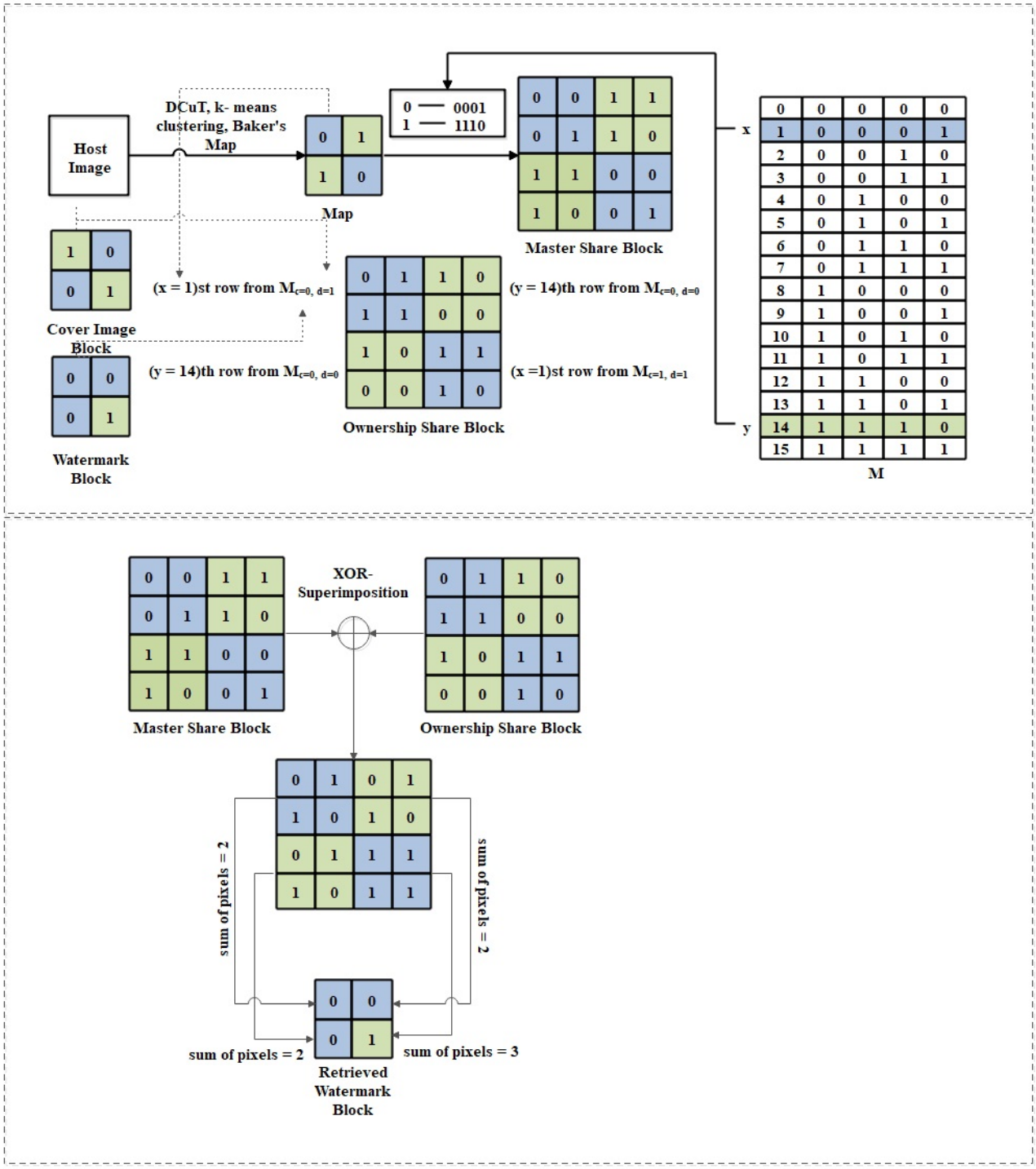


Figure 4.5: An Example to show (a) Construction of *OS* and (b) Superimposition of *IS* and *OS*

performance of the proposed scheme. The watermark size can be increased or decreased depending on the host image size. The number of blocks created in the host image should be equal to the watermark size. Figure 4.6 shows ten host images that are used for experimentation. Figure 4.7 shows the cover and watermark images used for experimentation.

(a) (b) (c) (d) (e)

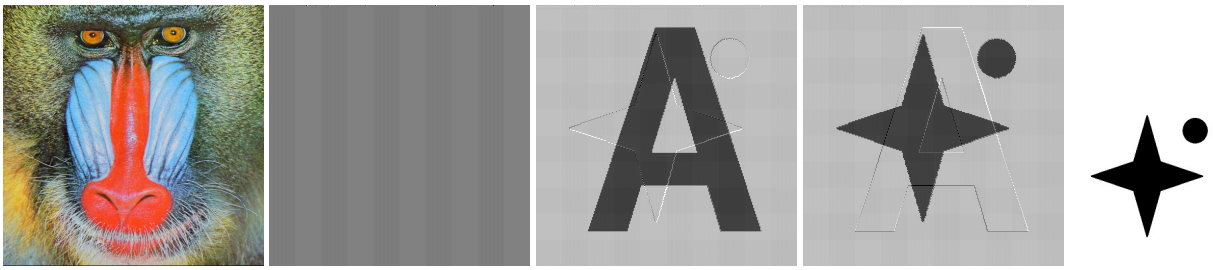
(f) (g) (h) (i) (j)

Figure 4.6: Different host images (a) Airplane (b) Barbara (c) Girl (d) Goldhill (e) House (f) Lake (g) Lena (h) Mandrill (i) Peppers (j) Zelda

(a) (b)

Figure 4.7: (a) Cover Image (b) Watermark

Figure 4.8 shows the results of the proposed scheme when applied on Mandrill image. Figure 4.8(c) shows the created noiseless OS. *XOR*-superimposition of MS (Figure 4.8(b)) and OS (Figure 4.8(c)) results into extracted watermark which is shown in Figure 4.8(d). This is further reduced to its original size, as demonstrated in Figure 4.8(e).



(a) (b) (c) (d) (e)

Figure 4.8: (a) Host Image (b) MS (c) OS (d) Extracted Watermark (e) Reduced Watermark

4.4.1 Computational Complexity of Proposed Scheme

Algorithm 4.1 takes $O(n^2 log\ n)$ time, which can be described as follows: Step 1 takes $O(n^2 log\ n)$ time with reference to Candès and Donoho (2004). Steps 2-5 take $O(4 \times n)$ time, as pre-processing is applied on every pixel of the image. Steps 6-8 take $O(3 \times (\frac{n}{bh \times bw}))$ time. The total complexity can be represented as,

$$Complexity = O(n^2 log\ n) + O(4 \times n) + O(3 \times (\frac{n}{bh \times bw})) = O(n^2 log\ n) \quad \ldots (4.11)$$

Similarly, Algorithm 4.2 takes $O(n^2 log\ n)$ time as the time complexities for step 1 and steps 2-6 are $O(n^2 log\ n)$ Candès and Donoho (2004) and $O(n)$, respectively. Step 8 takes $O(n)$ time as XOR-operation is performed on every share pixel.

Thus the total time complexity of the scheme is $O(n^2 log\ n)$, that is basically driven by *DCuT*.

4.4.2 Robustness Assessment

Various attacks have been applied on different images to test the robustness and the results are shown in Tables 4.1 and 4.2 for NC and BER, respectively. Following image manipulation attacks are performed on test images:

i. ***JPEG* Compression:** To test the robustness against *JPEG* Compression, the test images are compressed with quality (Q) factor values in the range 50-90. NC and BER values of the watermark retrieved is above 0.9998 and below 0.00016 respectively, for every test image, while SSIM value is around 1. Figure 4.9 shows the results for the Mandrill image where the compressed image is shown in Figure 4.9(a) with $Q = 90$ and PSNR = 33.45 *dB*, the superimposition result of MS and OS is shown in Figure 4.9(b) while Figure 4.9(c) shows the reduced watermark with NC = 1.00. All these results prove that the proposed scheme is robust against *JPEG* Compression attack.

ii. **Rotation Attack:** To test the robustness against rotation, the test images are rotated with angles (A) values in the range 10-50. NC and BER values of the watermark retrieved is above 0.9991 and below 0.00091 respectively, for every test image, while SSIM value is above 0.9999. Figure 4.10 shows the results for the Mandrill image where the rotated image is shown in Figure 4.10(a) with A = 60°and PSNR = 9.4488 *dB*, the superimposition result of MS and OS is

shown in Figure 4.10(b) while Figure 4.10(c) shows the reduced watermark with NC = 0.9993. All these results prove that the proposed scheme is robust against Rotation attack even when the attacked image has low PSNR.

iii. **Median Filtering Attack:** To test the robustness against Median Filtering Attack, the test images are attacked with window sizes (*ws*) of 2×2, 4×4 and 6×6. NC and BER values of the watermark retrieved is above 0.9999 and below 0.0003 respectively, for every test image, while SSIM value is above 0.9999. Figure 4.11 shows the results for the Mandrill image where the attacked image is shown in Figure 4.11(a) with $ws = 3 \times 3$ and PSNR = 20.4138 *dB*, the superimposition result of MS and OS is shown in Figure 4.11(b) while Figure 4.11(c) shows the reduced watermark with NC = 1. All these results prove that the proposed scheme is well robust against Media Filtering attack.

iv. **Cropping Attack:** To test the robustness against Cropping Attack, the test images are attacked with window sizes (*ws*) of 16×16, 64×64 and 256×256. NC and BER values of the watermark retrieved is above 0.9991 and below 0.00093 respectively, for every test image, while SSIM value is above 0.9999. Figure 4.12 shows the results for the Mandrill image where the cropped image is shown in Figure 4.12(a) with $ws = 128 \times 128$ and PSNR = 18.0368 *dB*, the superimposition result of MS and OS is shown in Figure 4.12(b) while Figure 4.12(c) shows the reduced watermark with NC = 0.9997. All these results prove that the proposed scheme is robust against Cropping attack.

v. **Gaussian Noise Attack:** To test the robustness against gaussian noise, the test images are attacked with this noise with mean 0 and variance (V) in the range 0.01 to 0.09. NC and BER values of the watermark retrieved is above 0.9997 and below 0.00076 respectively, for every test image, while SSIM value is 1. Figure 4.13 shows the results for the Mandrill image where the attacked image is shown in Figure 4.13(a) with $V = 0.09$, PSNR = 14.49 *dB*, the superimposition result of MS and OS is shown in Figure 4.13(b) while Figure 4.13(c) shows the reduced watermark with NC = 0.9999. All these results prove that the proposed scheme is robust against Gaussian Noise.

vi. **Poisson noise:** To test the robustness against Poisson noise, the test images are attacked with this noise where no artificial noise is added but it is added from the image itself. NC, BER and

SSIM values of the watermark retrieved is above 1, 0 and 1 respectively, for every test image. Figure 4.14 shows the results for the Mandrill image where the attacked image is shown in Figure 4.14(a) with PSNR = 27.0710 *dB*, the superimposition result of MS and OS is shown in Figure 4.14(b) while Figure 4.14(c) shows the reduced watermark with NC = 1. All these results prove that the proposed scheme is robust against Poisson Noise.

vii. **Salt and Pepper Noise:** To test the robustness against Salt and Pepper noise, the test images are attacked with this noise with noise density (D) in range 0.01 to 0.09. NC, BER and SSIM values of the watermark retrieved are around 0.9998, 0.0001 and 1 respectively, for every test image. Figure 4.15 shows the results for the Mandrill image where the attacked image is shown in Figure 4.15(a) with PSNR = 18.3490 *dB*, the superimposition result of MS and OS is shown in Figure 4.15(b) while Figure 4.15(c) shows the reduced watermark with NC = 1. All these results prove that the proposed scheme is robust against this attack.

viii. **Speckle Noise:** To test the robustness against Speckle Noise, the test images are attacked with variance (V) in range 0.01 to 0.10. NC and BER values of the watermark retrieved is above 0.9999 and below 0.00003 respectively, for every test image, while SSIM value is above 1. Figure 4.16 shows the results for the Mandrill image where the cropped image is shown in Figure 4.16(a) having PSNR = 18.5967 *dB*, the superimposition result of MS and OS is shown in Figure 4.16(b) while Figure 4.16(c) shows the reduced watermark with NC = 1.00. All these results prove that the proposed scheme is robust against this attack.

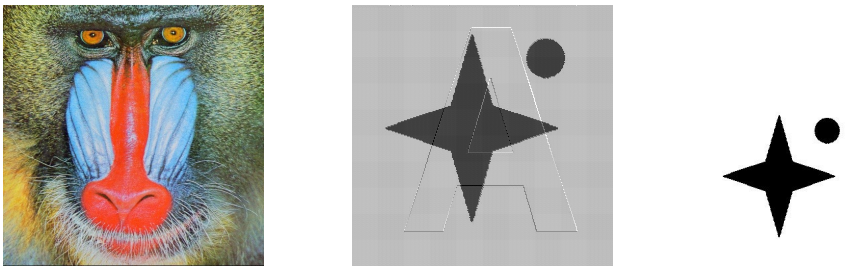
ix. **Sharpening Attack:** To test the robustness against sharpening, the test images are sharpened with different combinations of radius (R) and amount (A). NC and BER values of the watermark retrieved is above 0.9999 and below 0.000091 respectively, for every test image, while SSIM value is 1. Figure 4.17 shows the results for the Mandrill image where the sharpened image is shown in Figure 4.17(a) with PSNR = 18.2728 *dB*, the superimposition result of MS and OS is shown in Figure 4.17(b) while Figure 4.17(c) shows the reduced watermark with NC = 1. All these results prove that the proposed scheme is robust against sharpening.

x. **Sobel Attack:** When the image is attacked with sobel noise, the attacked image contains only detected edges. NC and BER values of the watermark retrieved is above 0.9983 and below 0.0023 respectively, for every test image, while SSIM value is above 0.9999. Figure 4.18 shows

the results for the Mandrill image where the attacked image is shown in Figure 4.18(a) having PSNR = 6.3443 *dB*, the superimposition result of MS and OS is shown in Figure 4.18(b) while Figure 4.18(c) shows the reduced watermark with NC = 0.9988. All these results prove that the proposed scheme is robust against sobel noise.

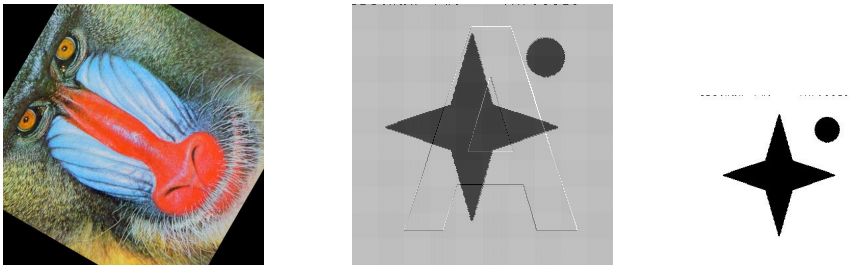
xi. **Blurring attack:** To test the robustness against Blurring, the test images are attacked with different radius (R) values. NC and BER values of the watermark retrieved is above 0.9999 and below 0.00012 respectively, for every test image, while SSIM value is 1. Figure 4.19 shows the results for the Mandrill image where the attacked image is shown in Figure 4.19(a) having PSNR = 17.5692 *dB*, the superimposition result of MS and OS is shown in Figure 4.19(b) while Figure 4.19(c) shows the reduced watermark with NC = 1.00. All these results prove that the proposed scheme is robust against blurring.

The observations discussed are shown in Table 4.1 from where the outstanding performance of the proposed scheme against various attacks and images for various ranges, can be analyzed. The NC values in every case is above 0.99 while BER values are close to 0 for every test image. This proves that the scheme is highly robust.



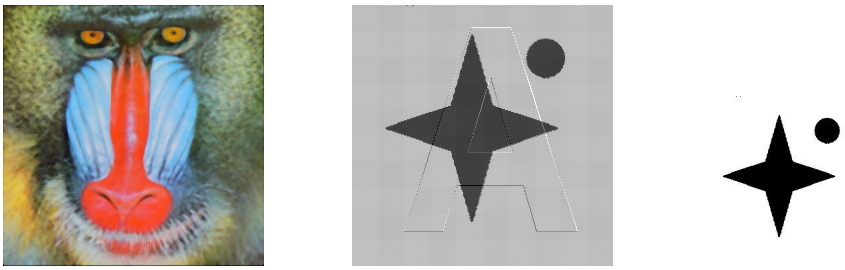
(a) (b) (c)

Figure 4.9: (a) Compressed Image (Q=90, PSNR = 33.45) (b) Superimposed Result (c) Reduced Watermark (NC = 1.00)



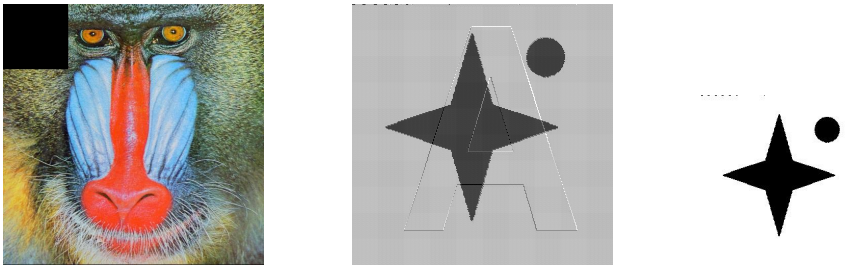
(a) (b) (c)

Figure 4.10: (a) Rotated Image (A=60°, PSNR = 9.4488) (b) Superimposed Result (c) Reduced Watermark (NC = 0.9993)



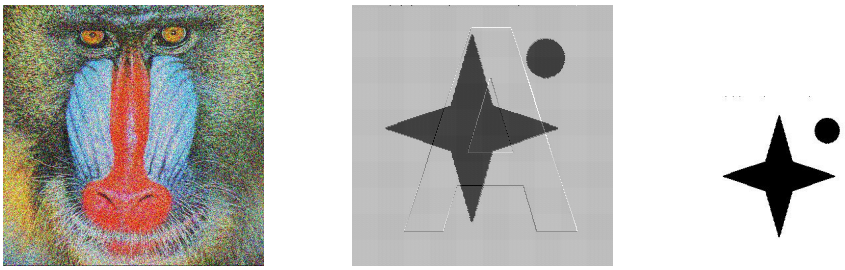
(a) (b) (c)

Figure 4.11: (a) Image after Median Filtering Attack ($ws = 3 \times 3$, PSNR = 20.4138) (b) Superimposed Result (c) Reduced Watermark (NC = 1.00)



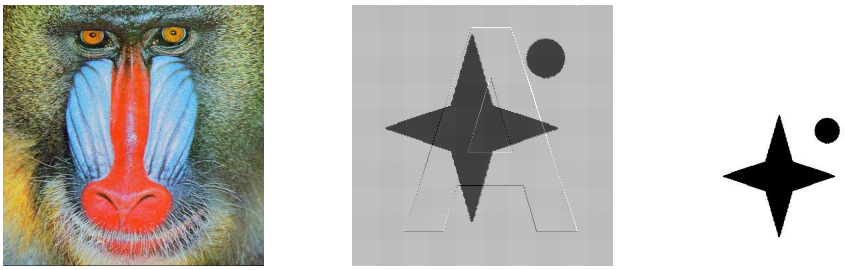
(a) (b) (c)

Figure 4.12: (a) Cropped Image ($cw = 128 \times 128$, PSNR = 18.0368) (b) Superimposed Result (c) Reduced Watermark (NC = 0.9997)



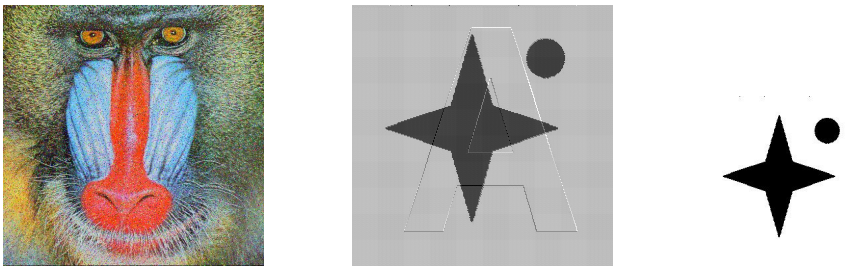
(a) (b) (c)

Figure 4.13: (a) Image with Gaussian Noise ($V = 0.09$, PSNR = 14.49) (b) Superimposed Result (c) Reduced Watermark (NC = 0.9999)



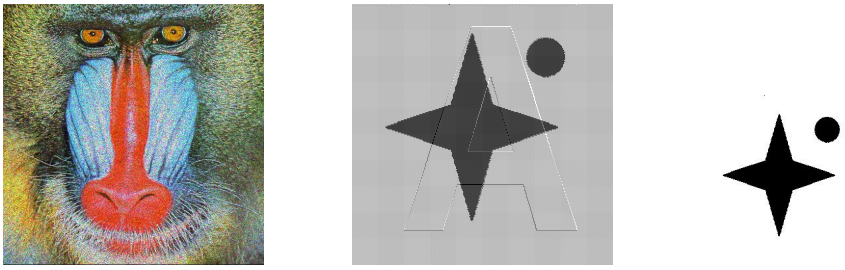
(a) (b) (c)

Figure 4.14: (a) Image with Poisson Noise (PSNR = 27.0710) (b) Superimposed Result (c) Reduced Watermark (NC = 1.00)



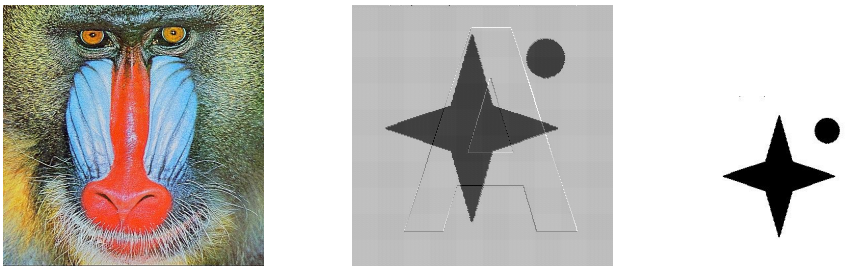
(a) (b) (c)

Figure 4.15: (a) Image with Salt and Pepper Noise (D = 0.09, PSNR = 18.3490) (b) Superimposed Result (c) Reduced Watermark (NC = 1.00)



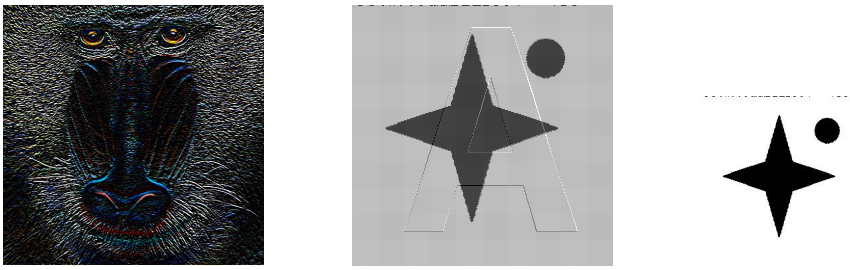
(a) (b) (c)

Figure 4.16: (a) Image with Speckle Noise, PSNR = 18.5967) (b) Superimposed Result (c) Reduced Watermark (NC = 1.00)



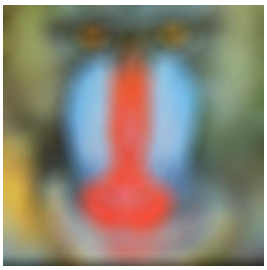
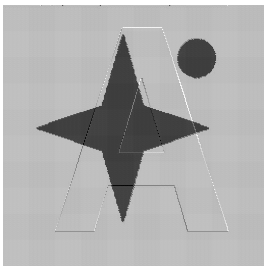
(a) (b) (c)

Figure 4.17: (a) Sharpened Image (R = 1, A = 2, PSNR = 18.2728) (b) Superimposed Result (c) Reduced Watermark (NC = 1.00)



(a) (b) (c)

Figure 4.18: (a) Image with Sobel Attack (PSNR=6.3443) (b) Superimposed Result (c) Reduced Watermark (NC = 0.9988)


(a) (b) (c)

Figure 4.19: (a) Blurred Image (R = 25, PSNR = 17.5692) (b) Superimposed Result (c) Reduced Watermark (NC = 1.00)

Table 4.1: NC Results for different images against different attacks

	Airplane	Barbara	Girl	Goldhill	House	Lake	Lena	Mandrill	Peppers	Zelda
JPEG Compression										
Q=50	1	1	1	1	1	0.99	1	1	1	1
Q=70	1	1	1	1	1	0.99	1	1	1	1
Q=90	1	1	1	1	1	0.99	1	1	1	1
Rotation										
A=10	0.9998	0.9996	0.9998	0.9996	0.9997	0.9998	0.9997	0.9997	0.9862	0.9993
A=30	0.9995	0.9993	0.9995	0.9988	0.9994	0.9995	0.9995	0.9994	0.9994	0.9991
A=50	0.9995	0.9993	0.9994	0.9988	0.9993	0.9994	0.9994	0.9993	0.9994	0.999
Median Filter										
$ws = 2 \times 2$	1	1	1	1	1	1	1	1	1	1
$ws = 4 \times 4$	1	1	1	1	1	1	1	1	1	1
$ws = 6 \times 6$	1	1	1	1	1	1	1	1	1	1
Cropping										
$cw = 16 \times 16$	1	1	1	0.9992	1	1	1	1	1	1
$cw = 64 \times 64$	0.9999	0.9999	1	0.9992	1	1	0.9999	0.9999	1	0.9999
$cw = 256 \times 256$	0.9993	0.9992	0.9992	0.9985	0.9992	0.9998	0.9991	0.9992	0.9992	0.999
Gaussian Noise										
V=0.01	1	1	1	1	1	1	1	1	1	1
V=0.04	1	1	1	0.9999	1	1	1	1	1	0.9997
V=0.07	1	0.9999	1	0.9998	1	1	1	0.9999	1	0.9997
V=0.09	1	0.9999	1	0.9997	1	1	1	0.9999	1	0.9997
Poisson Noise										
	1	1	1	1	1	1	1	1	1	1
Salt and Pepper Noise										
D=0.01	1	1	1	1	1	1	1	1	1	1
D=0.04	1	1	1	1	1	1	1	1	1	0.9999
D=0.07	1	1	1	0.9999	1	1	1	1	1	0.9998
D=0.09	1	1	1	0.9999	1	1	1	1	1	0.9998
Speckle Noise										
V=0.01	1	1	1	1	1	1	1	1	1	1

V=0.04	1	1	1	1	1	1	1	1	1	1
V=0.07	1	1	1	1	1	1	1	1	1	1
V=0.09	1	1	1	1	1	1	1	1	1	1
Sharpening										
(R=2, A=0.5)	1	1	1	1	1	1	1	1	1	1
(R=2, A=0.8)	1	1	1	1	1	1	1	1	1	1
(R=1, A=1.4)	1	1	1	1	1	1	1	1	1	1
(R=1, A=1.7)	1	1	1	1	1	1	1	1	1	1
Sobel										
	0.9983	0.9986	0.9977	0.9997	0.9988	0.9989	0.9983	0.9985	0.9985	0.9984
Blurring										
(R=10)	1	1	1	1	1	1	1	1	1	1
(R=20)	1	0.99	1	1	1	1	1	1	1	0.99

Table 4.2: BER Results for different Images against different attacks

	Airplane	Barbara	Girl	Goldhill	House	Lake	Lena	Mandrill	Peppers	Zelda
JPEG Compression										
Q=50	0	0	0	0	0	0.00016	0	0	0	0
Q=70	0	0	0	0	0	0.00016	0	0	0	0
Q=90	0	0	0	0	0	0.00016	0	0	0	0
Rotation										
A=10	0.00018	0.00038	0.00018	0.00044	0.00028	0.0003	0.00033	0.0003	0.00025	0.00065
A=30	0.00051	0.00059	0.0005	0.00094	0.00057	0.00061	0.00053	0.00065	0.00064	0.00093
A=50	0.00056	0.00068	0.00054	0.0012	0.0007	0.00065	0.00056	0.00073	0.00062	0.00093
Median Filter										
$ws = 2 \times 2$	0	0	0	0	0	0.000091	0	0	0	0.00003
$ws = 4 \times 4$	0	0	0	0.000015	0	0.000091	0	0.000015	0	0.000015
$ws = 6 \times 6$	0	0.000015	0	0.000015	0	0.000091	0	0.00003	0	0.000045
Cropping										
$cw = 16 \times 16$	0.000001	0.000015	0	0	0	0.00009	0	0	0	0.00003
$cw = 64 \times 64$	0.00006	0.000061	0.00003	0.000045	0.000045	0.00015	0.000061	0.000076	0.000045	0.00009
$cw = 256 \times 256$	0.00074	0.00077	0.00077	0.00093	0.0008	0.00086	0.0008	0.00082	0.00077	0.00099
Gaussian Noise										
V=0.01	0	0	0	0	0	0.000091	0	0	0	0.0001
V=0.04	0.000015	0.000045	0	0.0001	0.000015	0.000091	0.000015	0.00003	0	0.00024
V=0.07	0.000015	0.000076	0	0.00019	0.000015	0.000091	0.00003	0.000076	0	0.00028
V=0.09	0.000015	0.000076	0.000015	0.00027	0.00003	0.000091	0.000045	0.000076	0.000015	0.0003
Poisson Noise										
	0	0	0	0	0	0.00009	0	0	0	0.000015
Salt and Pepper Noise										
D=0.01	0	0	0	0	0	0.000091	0	0.000015	0	0.000015

D=0.04	0.000015	0.000015	0	0.000015	0.000015	0.000091	0.000015	0.00003	0	0.000091
D=0.07	0.000015	0.000045	0	0.0001	0.000015	0.000091	0.000015	0.00003	0	0.00016
D=0.09	0.000015	0.000045	0	0.00012	0.000015	0.000091	0.00003	0.000045	0.000015	0.00016
Speckle Noise										
V=0.01	0	0	0	0	0	0.000091	0	0	0	0
V=0.04	0.000015	0	0	0	0	0.000091	0.000015	0	0	0.000015
V=0.07	0.000015	0	0	0	0	0.000091	0.000015	0	0	0.000015
V=0.09	0.000015	0	0	0.000015	0.000015	0.000091	0.000015	0.000015	0	0.000015
Blurring										
(R=10)	0.000015	0.000015	0	0	0	0.000091	0.000015	0.000015	0	0.000015
(R=20)	0.000015	0.00006	0	0.000015	0.000015	0.000091	0.00003	0.000045	0.000015	0.000076

The proposed scheme is compared with the existing scheme on different images against different attacks and the results are shown in Table 4.3.

Table 4.3: Comparison of Proposed Scheme with existing schemes for different images and at various attacks

Images		Rawat and Raman (2012)	Hou and Huang (2012)	Hou et al. (2016)	Devi et al. (2016)	Abraham and Paul (2019)	Roy and Pal (2017)	Murali and Sankaradass (2018)	Ernawan and Kabir (2020)	Hurrah et al. (2019)	Thanki et al. (2019)	Proposed Scheme
JPEG Compression												
Lena	Q=10	-	0.59	-	-	-	-	0.85	-	-	-	1
	Q=20	-	0.6	-	-	0.7362	-	0.85	-	-	-	1
	Q=50	0.9611	-	-	0.9804	0.8873	-	-	-	-	-	1
	Q=70	0.9648	-	-	0.9873	0.8314	-	-	-	-	-	1
	Q=90	0.9772	-	-	0.9931	-	-	-	-	-	-	1
Airplane	Q=5	-	0.9943	0.9944	-	-	-	-	-	-	-	1
	Q=50	0.9631	-	-	0.9797	-	-	-	-	-	-	1
	Q=70	0.9697	-	-	0.9987	-	-	-	-	-	-	1
	Q=90	0.9814	-	-	0.9934	-	-	-	-	-	-	1
Lake	Q=10	-	0.6	-	-	-	-	0.87	-	-	-	1
	Q=20	-	0.61	-	-	-	-	0.89	-	-	-	1
Mandrill	Q=10	-	0.6	-	-	-	-	0.81	-	-	-	1
	Q=20	-	0.63	-	-	-	-	0.82	-	-	-	1
House	Q=10	-	0.62	-	-	-	-	0.8	-	-	-	1
	Q=20	-	0.63	-	-	-	-	0.81	-	-	-	1
Goldhill	Q=50	0.9592	-	-	0.9946	-	-	-	-	-	-	1
	Q=70	0.9667	-	-	0.9948	-	-	-	-	-	-	1
	Q=90	0.9765	-	-	0.9973	-	-	-	-	-	-	1
Peppers	Q=40	-	0.97	-	-	-	0.6978	-	0.661	-	0.9597	1
	Q=50	-	-	-	-	-	0.7502	-	0.6382	-	0.9639	1
	Q=60	-	-	-	-	-	0.8067	-	0.6087	-	0.9741	1

Table 4.3 Continued..

Images		Rawat and Raman (2012)	Hou and Huang (2012)	Hou et al. (2016)	Devi et al. (2016)	Abraham and Paul (2019)	Roy and Pal (2017)	Murali and Sankaradass (2018)	Ernawan and Kabir (2020)	Hurrah Hurrah et al. (2019)	Thanki et al. (2019)	Proposed Scheme
	Q=70	-	-	-	-	-	0.8916	-	0.5876	-	0.9837	1
	Q=80	-	-	-	-	-	0.9404	-	0.6069	-	0.9898	1
	Q=90	-	-	-	-	-	0.9639	-	0.637	-	0.991	1
Rotation												
Lena	A=1	0.8549	-	-	0.9382	-	-	-	-	-	-	0.9999
	A=5	0.7353	-	-	0.9589	-	-	-	-	-	-	0.9999
	A=20	-	0.52	-	-	-	-	0.79	-	-	-	0.9991
Airplane	A=1	0.7927	-	-	0.9331	-	-	-	-	-	-	0.9999
	A=5	0.7021	-	-	0.9587	-	-	-	-	-	-	0.9999
Peppers	A=20	-	-	-	-	-	0.5593	-	0.5864	-	-	0.9991
	A=45	-	-	-	-	-	0.5521	-	-	-	-	0.9889
Lake	A=20	-	0.56	-	-	-	-	0.78	-	-	-	0.9998
Mandrill	A=20	-	0.54	-	-	-	-	0.79	-	-	-	0.9998
House	A=20	-	0.5	-	-	-	-	0.8	-	-	-	0.9998
Goldhill	A=1	0.8493	-	-	0.9826	-	-	-	-	-	-	0.9999
	A=5	0.6992	-	-	0.9797	-	-	-	-	-	-	0.9999
Median Filtering												
Lena	$ws = 2 \times 2$	-	0.61	-	-	-	-	0.95	-	-	-	1
	$ws = 3 \times 3$	0.9514	-	-	0.979	-	-	-	-	-	-	1
	$ws = 5 \times 5$	0.9379	-	-	0.9606	-	-	-	-	-	-	1
	$ws = 7 \times 7$	0.9279	-	-	0.9484	-	-	-	-	-	-	1
Lake	$ws = 2 \times 2$	-	0.61	-	-	-	-	0.87	-	-	-	1
Mandrill	$ws = 2 \times 2$	-	0.54	-	-	-	-	0.89	-	-	-	1
House	$ws = 2 \times 2$	-	0.63	-	-	-	-	0.85	-	-	-	1
Airplane	$ws = 3 \times 3$	0.9638	-	-	0.9873	-	-	-	-	-	-	1
	$ws = 5 \times 5$	0.9421	-	-	0.9724	-	-	-	-	-	-	1
	$ws = 7 \times 7$	0.925	-	-	0.9577	-	-	-	-	-	-	1
Goldhill	$ws = 3 \times 3$	0.9499	-	-	0.9912	-	-	-	-	-	-	1
	$ws = 5 \times 5$	0.9299	-	-	0.9851	-	-	-	-	-	-	1
	$ws = 7 \times 7$	0.9187	-	-	0.9807	-	-	-	-	-	-	1
Peppers	$ws = 3 \times 3$	-	-	-	-	-	0.8055	-	-	-	-	0
	$ws = 5 \times 5$	-	-	-	-	-	0.3721	-	-	-	-	0
	$ws = 7 \times 7$	-	-	-	-	-	0.407	-	-	-	-	0.000015
Cropping												
Lena	%C=20	0.8481	-	-	0.8261	-	-	-	-	-	-	1
	%C=25	-	-	-	-	0.75	-	-	-	1	-	1
	%C=40	0.842	-	-	0.7897	-	-	-	-	-	-	0.9999
	%C=50	-	0.79	0.92	0.7333	0.5	-	-	-	0.998	-	0.9999
	%C=60	0.7863	-	-	-	-	-	-	-	-	-	0.9998
	%C=75	-	-	-	-	0.25	-	-	-	0.989	-	0.9997
Airplane	%C=20	0.7243	-	-	0.7333	-	-	-	-	-	-	1
	%C=40	0.7458	-	-	0.7192	-	-	-	-	-	-	0.9999

Table 4.3 Continued..

Images		Rawat and Raman (2012)	Hou and Huang (2012)	Hou et al. (2016)	Devi et al. (2016)	Abraham and Paul (2019)	Roy and Pal (2017)	Murali and Sankaradass (2018)	Ernawan and Kabir (2020)	Hurrah Hurrah et al. (2019)	Thanki et al. (2019)	Proposed Scheme
	%C=60	0.686	-	-	0.7285	-	-	-	-	-	-	0.9998
Peppers	%C=11	-	0.99	-	-	-	-	-	-	-	-	1
	%C=50	-	0.8415	0.8473	-	-	0.9657	-	-	-	-	0.9999
Mandrill	%C=50	-	0.81	0.99	-	-	-	-	-	-	-	0.9999
House	%C=50	-	0.83	0.8	-	-	-	-	-	-	-	0.9999
Lake	%C=50	-	0.85	0.82	-	-	-	-	-	-	-	0.9999
Goldhill	%C=20	0.7814	-	-	0.8969	-	-	-	-	-	-	1
	%C=40	0.8049	-	-	0.8054	-	-	-	-	-	-	0.9999
	%C=60	0.7177	-	-	0.728	-	-	-	-	-	-	0.9998
Gaussian Noise												
Lena	V=0.01	0.8374	0.53	-	0.9318	-	-	0.89	-	-	-	1
	V=0.03	0.7761	-	-	0.8981	-	-	-	-	-	-	1
	V=0.05	0.7556	-	-	0.874	-	-	-	-	-	-	1
Airplane	V=0.01	0.832	-	-	0.9267	-	-	-	-	-	-	1
	V=0.03	0.7663	-	-	0.8859	-	-	-	-	-	-	1
	V=0.05	0.7602	0.9085	0.9548	0.8691	-	-	-	-	-	-	1
Mandrill		-	0.58	-	-	-	-	0.83	-	-	-	1
House		-	0.55	-	-	-	-	0.82	-	-	-	1
Lake		-	0.54	-	-	-	-	0.9	-	-	-	1
Goldhill	V=0.01	0.8564	-	-	0.9755	-	-	-	-	-	-	1
	V=0.03	0.7902	-	-	0.9599	-	-	-	-	-	-	1
	V=0.05	0.7751	-	-	0.9475	-	-	-	-	-	-	0.9998
Peppers	V=0.01	-	-	-	-	-	0.6412	-	-	-	-	1
	V=0.02	-	-	-	-	-	0.6075	-	-	-	-	1
	V=0.1	-	-	-	-	-	0.5569	-	-	-	-	1
Sharpening												
Lena	alpha=0.1	0.8688	0.75	-	0.9208	0.9455	-	0.87	-	0.975	-	1
Airplane	alpha=0.1	0.8906	0.9249	0.9255	0.9357	-	-	-	-	-	-	1
Peppers	alpha=0.1	-	0.96	-	-	-	0.9645	-	-	-	-	1
Lake	alpha=0.1	-	0.76	-	-	-	-	0.92	-	-	-	1
Mandrill	alpha=0.1	-	0.79	-	-	-	-	0.83	-	-	-	1
House	alpha=0.1	-	0.79	-	-	-	-	0.83	-	-	-	1
Goldhill	alpha=0.1	0.8737	-	-	0.9658	-	-	-	-	-	-	1
Lightening												
Airplane	20%	-	0.9943	0.9952	-	-	-	-	-	-	-	1
Peppers	20%	-	1	-	-	-	-	-	-	-	-	1
Darkening												
Airplane	20%	-	0.9939	0.9939	-	-	-	-	-	-	-	1
Peppers	20%	-	1	-	-	-	-	-	-	-	-	1
Blurring												
Peppers		-	0.99	-	-	-	0.5316	-	-	-	-	1

Table 4.3 Continued..

Images		Rawat and Raman (2012)	Hou and Huang (2012)	Hou et al. (2016)	Devi et al. (2016)	Abraham and Paul (2019)	Roy and Pal (2017)	Murali and Sankaradass (2018)	Ernawan and Kabir (2020)	Hurrah Hurrah et al. (2019)	Thanki et al. (2019)	Proposed Scheme
Salt and Pepper Noise												
Lena		-	0.58	-	-	0.97	-	0.89	-	0.96	-	1
Lake		-	0.59	-	-	-	-	0.91	-	-	-	1
Mandrill		-	0.59	-	-	-	-	0.81	-	-	-	1
House		-	0.58	-	-	-	-	0.82	-	-	-	1
Peppers			-	-	-	-	0.5852	-	-	-	-	1
Speckle Noise												
Lena		-	-	-	-	0.91	-	-	-	0.97	-	1
Poisson Noise												
Lena		-	-	-	-	0.9713	-	-	-	0.96	-	1

The '-' in the table refers that the values for those cells are not available in the referred works.

Table 4.3 shows that NC value of the attacked images is quite low in the existing schemes as compared to the proposed scheme. The results have been shown for various images affected by a variety of attacks. This higher robustness is ensured by the use of inner sub-bands of DCuT coefficients.

4.4.3 Security Analysis

In the proposed scheme, meaningful shares are created using the proposed codebook. These meaningful shares are stored with the TA that ensures security, as these shares are similar to the cover images and hence create no suspicion of some secret information being shared or stored.

Also, before shares are created, the watermark and coefficient matrices are scrambled using Baker Map, to enhance the security.

4.5 Conclusion of the Chapter

Multimedia Data and medical images are used on devices having low computation power. Due to computational constraints, watermarking schemes with less complexity are required. Thus, in this paper, a new secure and robust copyright protection scheme based on DCuT, *k*-means Clustering and *EVCS* is proposed. The selection of non fine scale layer DCuT coefficients enhance the

robustness of the scheme. Baker Map is used for scrambling host image and watermark to make the scheme secure. A codebook is proposed to create meaningful *OS*, thereby ensuring security of the scheme. The complexity of scheme is very low as watermark can be retrieved blindly just by *XOR*-superimposition of the shares. Experiments have been performed on different images by doing different attacks to check robustness of the scheme. *NC* value of the extracted watermark is maintained at 0.99 or more, which shows that the scheme has outstanding resistance to attacks. The advantages of the proposed scheme are high robustness, imperceptibility, security and blind detection. The watermark's size is not restricted to the size of the protected image. Comparison with the state-of-art copyright protection schemes reveals that the proposed scheme gives better performance. This scheme can be extended to multiple color images with multiple owners.

CHAPTER 5

Enhanced Curvelet Transform based Robust Copyright Protection Scheme for Color Images using Henon Map

.

5.1 Introduction

The Curvelet based copyright protection scheme showed high robustness and security, but the issue of false positives existed, *i.e.* apart from the rightful owner, other false entities can also prove their copyright on the image. Thus to handle this issue, the previous scheme was further extended. In this proposed scheme, six-scale layers are generated from Y component of host image by applying *DCuT* on it. *MS* is constructed using the non fine scale layers. This share is then scrambled using Henon map to enhance security. The proposed scheme uses two watermarks. One watermark is

Contents of the work presented in this Chapter have been published in *Multimedia Tools and Applications*, Vol. 79, pp. 26155–26179, 2020 (SCI Indexed)

provided by the user while the other watermark is constructed using C_b and C_r components of the host image. The purpose of the second watermark is to handle the false positive cases. *MS*, two watermarks and cover image are used to construct Meaningful *OS* using *EVCS*. The ownership is proved when watermark is retrieved when *MS* is superimposed with *OS*. It can be observed from the experimental results that the proposed scheme can verify the copyright of the digital images, robust against several image processing attacks and handles false positive cases efficiently. The existing copyright protection scheme is compared with the proposed scheme and the results prove the proposed scheme performs better.

5.2 Background

This section discusses YC_bC_r Color Space and Henon Map Transform, that are used in the proposed scheme.

5.2.1 YC_bC_r Color Space

In YC_bC_r color space, Y refers to luminance component *i.e.* brightness (luma) while C_b and C_r are the chrominance actors, *i.e.* C_b is luma subtracted from blue color $(B-Y)$ and C_r luma subtracted from red color $(R-Y)$. YC_bC_r color space represents color using brightness and color difference signals, while *RGB* represents color as using red, green and blue components. The transformations between *RGB* and YC_bC_r color space in equations 5.1 and 5.2 :

$$\begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} = \begin{bmatrix} 0.29890 & 0.58660 & 0.11450 \\ -0.16874 & -0.33126 & 0.50000 \\ 0.50000 & -0.41869 & -0.8131 \end{bmatrix} \times \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad \ldots(5.1)$$

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1.40200 \\ 1 & -0.34414 & -0.71414 \\ 1 & 1.7720 & 0 \end{bmatrix} \times \begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} \quad \ldots(5.2)$$

5.2.2 Henon Map Transform

A Henon map is a chaotic 2D system with quadratic non-linearity where a point (x_n, y_n) is mapped to a new point in the same plane Hénon (1976) using following equations:

$$x_{n+1} = 1 - a \times x_n^2 + y_n \quad \ldots(5.3)$$

$$y_{n+1} = b \times x_n \quad \ldots(5.4)$$

The map is based on two parameters, a and b which decide the map behavior. The map behaves periodically and converges to a constant value. It diverges to infinity when $a = 1.4, b = 0.3$.

Various scrambling methods have been reviewed in Agarwal (2018). This analysis proves that Henon Transform scrambles data better as compared to Arnold Transform. *PSNR* of the image scrambled by Henon Transform is low as compared to the scrambled image obtained from Arnold Transform. Also, Henon Transform is quite faster as compared to Arnold Transform.

5.3 Proposed Scheme

In this section, the proposed copyright protection scheme is described. To enhance the security and improve robustness of the proposed watermarking scheme, Henon map is applied to both the image and watermark. The scheme is divided into two phases: Master-Ownership share construction; Identification Share construction. During the Master-Ownership share construction, the Y channel of the color image is used to generate the *MS* while C_r and C_b channels are used to create a watermark (W_2). *DCuT via* Wrapping is applied on Y channel of the image. As human eyes are more sensitive to low frequency information than to high frequency, the non fine scale layers are used to construct the *MS* that enhances robustness of the scheme. *MS* is constructed using K-means Clustering Technique. This constructed *MS* along with *WI* provided by user and W_2 are used to construct *OS* by *EVCS*.

Two watermarks are used to ensure no false positive cases. Both the watermarks are used to create a single *OS*, in such a way that when the *OS* is superimposed with *MS*, *WI* is retrieved while when its superimposed with rotated *MS*, W_2 is retrieved. The rotation in *MS* is performed by 90°in anti clockwise direction. If only *WI* is used, some false positive cases exist where the shares constructed from the images apart from the host image can also help in retrieving the watermark. If

only W_2 is used, the scheme would not have any external watermark image for protection, which would affect robustness of the scheme and also, it would be against the concept of watermarking based copyright protection scheme. Implementation of these two phases are shown in Figures 5.1 and 5.2.

5.3.1 Master-Ownership Share Construction

The steps for this phase are described in Algorithm 5.1. The *MS* is constructed from the Y channel of the color image, as this channel contains the maximum and sufficient information of the image. The other two channels of the image, *i.e.* C_r and C_b are used to construct W_2 to handle false positive cases.

After applying curvelet transform on the Y channel of the image, the inner non fine scale layers are used for the construction to ensure robustness of the scheme. These coefficients are divided into blocks which are further divided into two clusters to create a binary *MS*. This *MS* along with *WI*, W_2 and a cover image *CI* is used to create a meaningful *OS*. The codebooks used for this construction are given in Figure 5.4, where *WI* and w_2 represent the corresponding watermark bits of WI and W_2, W and B represent to white and black pixels respectively and CI_{bit} represents the corresponding binary bit in the cover image.

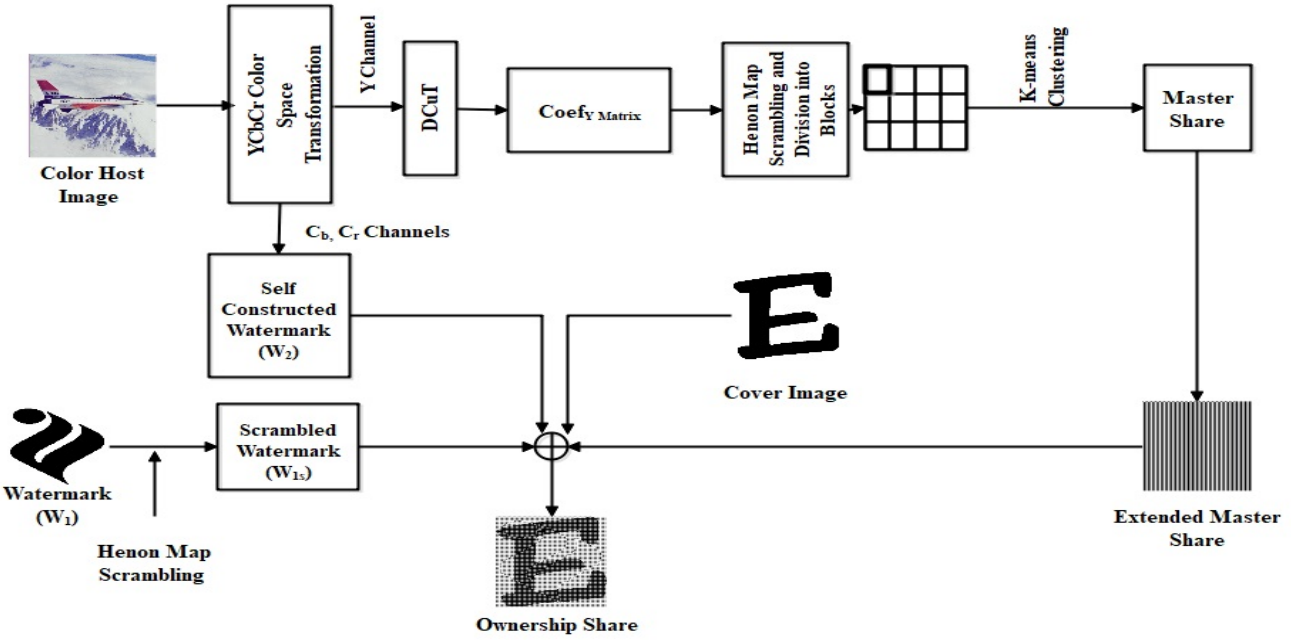


Figure 5.1: Block Diagram for Master-Ownership Share Generation

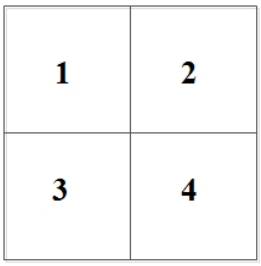


Figure 5.2: Four Divided Regions in the *MS*

Figure 5.3: 2×2 patterns for (a) Black and (b) White pixel

Algorithm 5.1 Generation of *MS* and *OS*

Input: *HI* of size $hh \times hw$, *CI* of size $ch \times cw$, *WI* of size $wh \times ww$
Output: *MS* and *OS*

1: Transform the host image in *RGB* color space to the YC_bC_r color space. C_b and C_r channels are utilized to create the watermark. Both the channels are binarized using Otsu's threshold Otsu (1979) and then an *XOR* operation is performed between them to construct a watermark (W_2). This self constructed watermark helps in dealing with false positive cases.
2: Apply Curvelet decomposition on Y channel to get its coefficient matrix. Extract the non-fine scale layers of this coefficient matrix and store into $CoefY$. These are used to create MS.
3: Scramble the coefficient matrix and WI using Henon Map Based Transform to ensure randomness and security.
4: Divide the coefficient matrix $CoefY$ into b_i blocks of size $bh \times bw$, where $i = 1$ to nb, $nb = \frac{hh \times hw}{bh \times bw}$, $bh = \frac{hh}{N_w}$, $bw = \frac{hw}{N_w}$ The matrix of blocks is represented as $yblock_i$
5: Classify the blocks into 2 clusters: Cluster 1 and Cluster 2, using K-means clustering.
$$MasterShare = kmeans(CoefY, 2)$$
The *MS* contains cluster number for every corresponding block *i.e.* 0 or 1. Size of map $= mh \times mw$, where $mh = \frac{hh}{bh}$ and $mw = \frac{hw}{bw}$. Size of map should be equal to the size of *WI* and W_2.
6: Construct an extended master share (EMS) of four times the size of MS, *i.e.* $4mh \times 4mw$. EMS is segmented into four equal regions as shown in Figure 5.2. In the region 1 of EMS, MS is placed by representing its white and black pixels with the 2×2 block patterns given in Figure 5.3. The patterns in other three regions can be defined according to the region 1, such that EMS(j,N_w-i-1) of region 2, EMS(N_w-j-1,i) of region 3 and EMS(N_w-i-1,N_w-j-1) of region are mapped to EMS(i,j) of region 1.
7: Construct OS using EMS, *WI*, W_2 and CI by following the codebook given in Figure 5.4. The size of OS would be equal to the size of MS.

After the construction of OS, *WI* is kept secretly by the copyright owner and the OS is registered to a TA for further authentication.

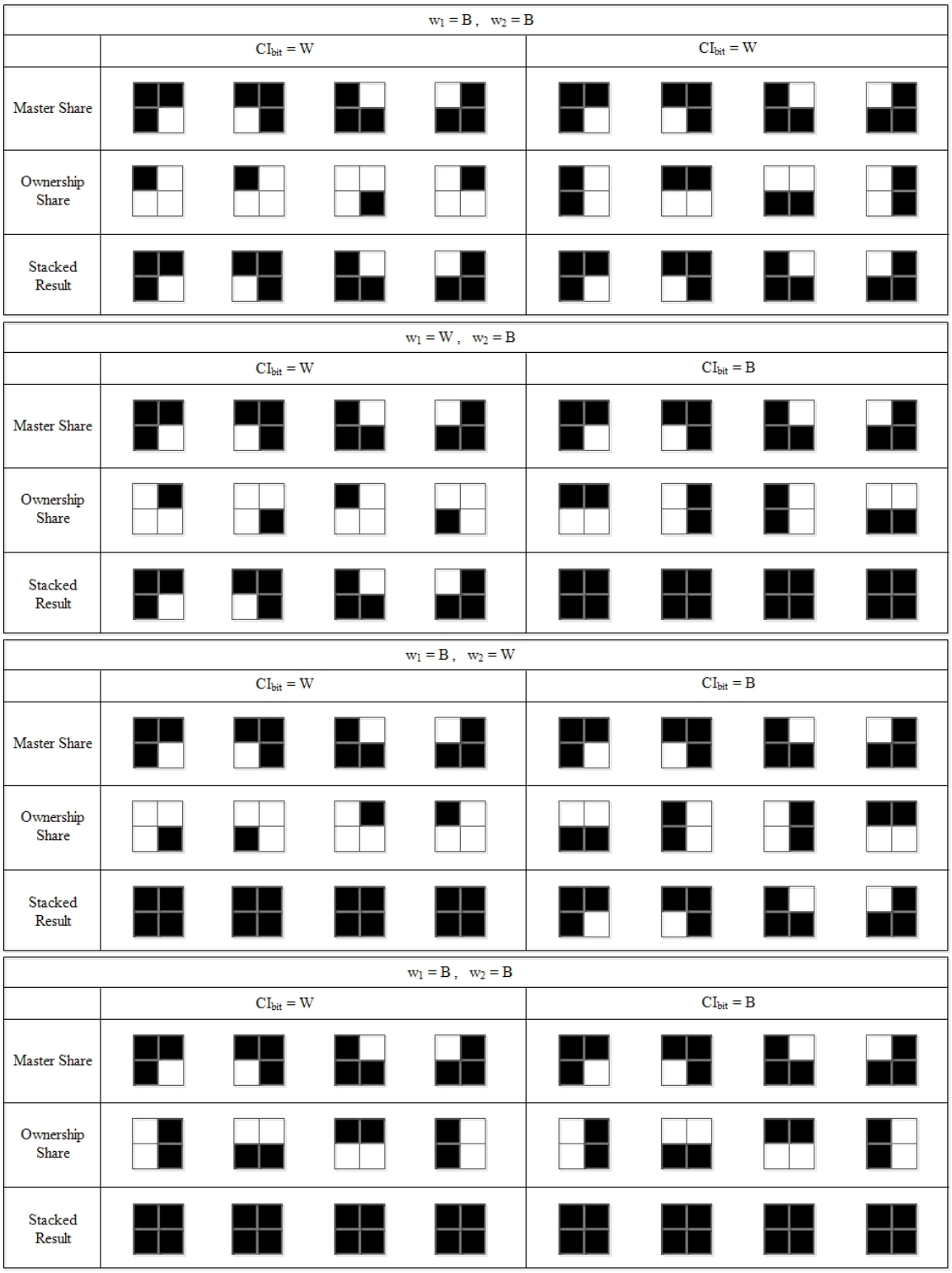


Figure 5.4: Codebook for Construction of OS

5.3.2 Identification Share Construction

Steps for this phase are described in Algorithm 5.2. When the copyright of the image has to be claimed, a MS is constructed from its Y channel using the algorithm followed in the previous phase and the OS is retrieved from TA. The superimposition result of OS with MS and the MS rotated by 90°in anticlockwise direction, should be similar to WI and W_2 respectively, to prove the copyright.

Algorithm 5.2 Generation of Identification Share

Input: Attacked Host Image (HI') of size $hh \times hw$
Output: Identification Share (IS)

1: Transform the host image in RGB color space to the YC_bC_r color space. C_b and C_r channels are utilized to create the watermark. Both the channels are binarized using Otsu's threshold Otsu (1979) and then an XOR operation is performed between them to construct a watermark ($W_2^{'}$).
2: Apply Curvelet decomposition on Y channel to get its coefficient matrix. Extract the non-fine scale layers of this coefficient matrix and store into $CoefY'$. These are used to create MS'.
3: Scramble the coefficient matrix using Henon Map Based Transform. Divide the coefficient matrix $CoefY$ into b_i blocks of size $bh \times bw$, where i = 1 to nb, $nb = \frac{hh \times hw}{bh \times bw}$, $bh = \frac{hh}{N_w}$, $bw = \frac{hw}{N_w}$ The matrix of blocks is represented as $yblock_i^{'}$.
4: Classify the blocks into 2 clusters: Cluster 1 and Cluster 2, using k-means clustering.
$$IdenificationShare = kmeans(CoefY', 2)$$
The identification share contains cluster number for every corresponding block *i.e.* 0 or 1.
5: Construct an extended identification share (EIS) of four times the size of MS, *i.e.* $4mh \times 4mw$. EIS is segmented into four equal regions as shown in Figure 5.2. In the first part of EIS, IS is placed by representing its white and black pixels with the 2×2 block patterns given in Figure 5.3. The patterns in other three regions can be defined according to the first region, such that EIS(j,N_w-i-1) of region 2, EIS(N_w-j-1,i) of region 3 and EIS(N_w-i-1,N_w-j-1) of region are mapped to EIS(i,j) of region 1.
6: Retrieve OS from CA and superimpose with EIS to retrieve TW_1. Then EIS is rotated by 90°in anticlockwise direction and superimposed with OS to retrieve TW_2. Both TW_1 and $TW_2$are divided into blocks of size 2×2, and for every block if count of black pixels is greater or equal than 2, it is represented by black else by white in WI' and $W_2^{'}$. These retrieved watermarks can be compared with WI and W_2 to prove the copyright.

5.4 Experimental Results and Discussion

The performance of the proposed scheme for color images is investigated through a set of experiments performed using MATLAB (R2018a), 64-bit (win64) software, on 228 different *8*-bit host images of size 512×512 and binary watermark image of size 256×256. Size of watermark is not fixed and can be adjusted as per the user requirement. Number of blocks created for the image should be equal to the size of watermark. Ten test images *viz.* Airplane, Barbara, Girl, Goldhill, House, Lake,

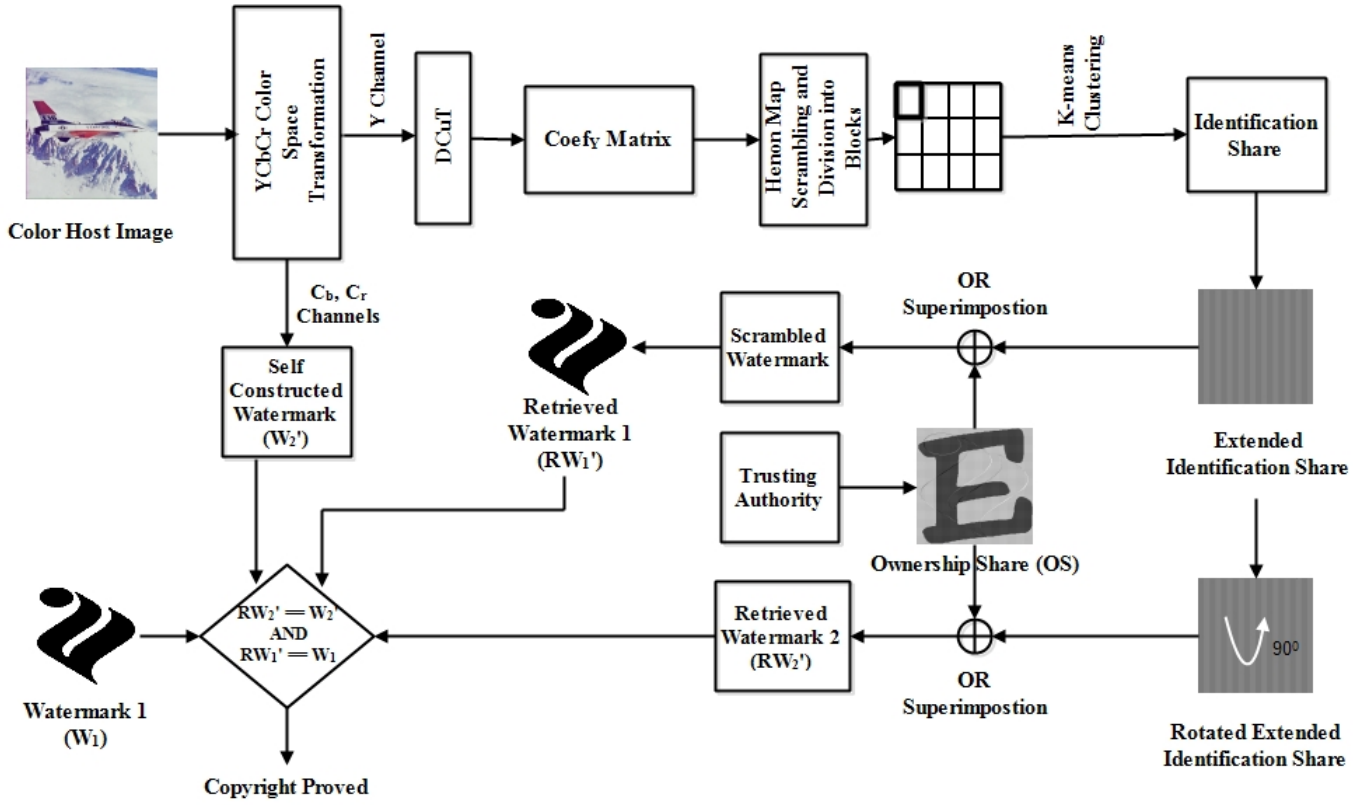
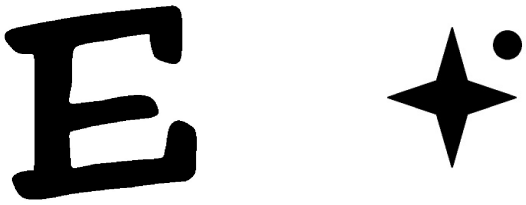


Figure 5.5: Block Diagram for Identification Share Generation

Lena, Mandrill, Peppers and Zelda are used for experimentation and presented in Figure 5.6. The cover image and watermark used for experimentation are shown in Figure 5.7.

Figure 5.6: Different input test images used in the proposed scheme (a) Airplane (b) Barbara (c) Girl (d) Goldhill (e) House (f) Lake (g) Lena (h) Mandrill (i) Peppers (j) Zelda

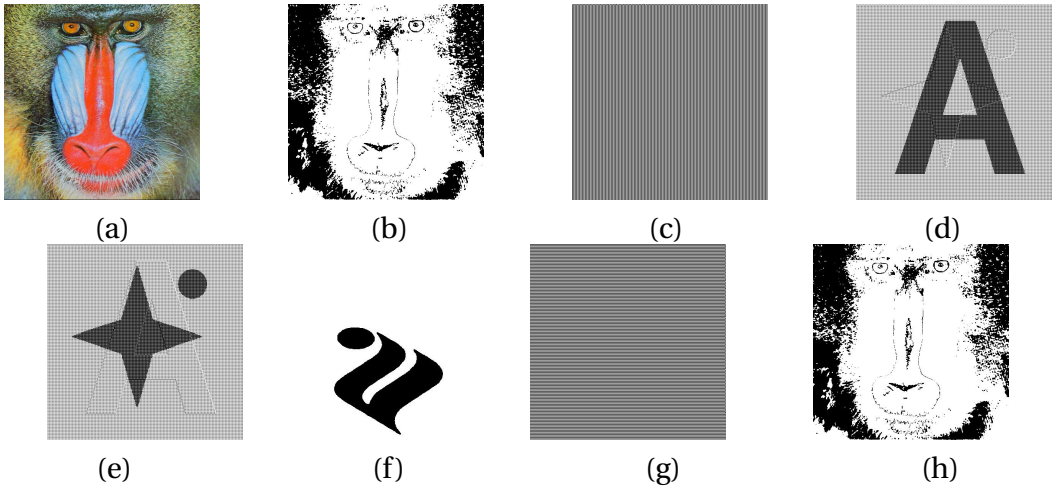
The implementation results of the proposed scheme are shown in Figure 5.8 for Mandrill image. Figure 5.8(b) represents the self constructed watermark that is constructed from C_b and C_r channels of the host image. Figure 5.8(c) represents the MS constructed using Y channel of host image. Figure 5.8(d) represents the meaningful ownershsip share constructed using Figure 5.8(b),



(a) (b)

Figure 5.7: Test Cover Image and Watermark (a) Cover Image: letter E (b) Watermark: Logo

Figure 5.8(c), Figure 5.7(a) and Figure 5.7(b). Figure 5.8(g) represents the rotated MS that is created by rotating Figure 5.8(c) by 90°in anti clockwise direction. When Figure 5.8(d) is superimposed with Figure 5.8(c), the watermark is received to prove the copyright, which is shown in Figure 5.8(e), while when Figure 5.8(d) is superimposed with Figure 5.8(g), the other watermark is received shown in Figure 5.8(h) that helps in handling false positive cases.



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 5.8: (a) Host Image (b) Self Constructed Watermark (c) MS (d) OS (d) Superimposed Result of MS and OS (e) Reduced Watermark (f) Rotated MS (g) Superimposed Result of Rotated MS and OS

5.4.1 Robustness Assessment

Robustness tests of the proposed scheme on different images against various attacks are shown in Tables 5.1 and 5.2 with respect to NC and BER, respectively. The values have been recorded for different parameter values of eveery attack, and the average value is presented in the Tables 5.1 and 5.2. The robustness results have been shown with respect to *WI*, as it is solely responsible or the robustness of the scheme. The image manipulation attacks performed on test images are as follows:

i. ***JPEG* Compression:** The test images have been compressed with quality (*Q*) factor ranging

from 10 to 90. NC and BER of retrieved watermark is above 0.9998 and below 0.00016 respectively, for all test images. SSIM of extracted watermark is 1 for all test images. This shows the proposed scheme is robust against this attack.

ii. **Rotation Attack:** The test images are rotated with angles (A) of 10°to 100°. NC and BER of retrieved watermark is above 0.9991 and below 0.00091 respectively, for all test images. SSIM of extracted watermark is above 0.9999 for all test images. This shows the proposed scheme is robust against this attack.

iii. **Median Filtering Attack:** The test images are applied filtering attack for window sizes (ws) of 2×2 to 10×10. NC and BER of retrieved watermark is above 0.9999 and below 0.0003 respectively, for all test images. SSIM of extracted watermark is 1 for all test images. This shows the proposed scheme is robust against this attack.

iv. **Cropping Attack:** The test images are cropped for window size 16×16,32×32, 64×64, 128×128, and 256×256. NC and BER of retrieved watermark is above 0.9991 and below 0.00093 respectively, for all test images. SSIM of extracted watermark is above 0.9999 for all test images. This shows the proposed scheme is robust against this attack.

v. **Gaussian Noise Attack:** The gaussian noise is added to the test images with mean 0 and variance (V) ranging from 0.01 to 0.10. NC and BER of retrieved watermark is above 0.9997 and below 0.00076 respectively, for all test images. SSIM of extracted watermark is 1 for all test images. This shows the proposed scheme is robust against this attack.

vi. **Poisson noise:** The noise is added from the image data itself instead of adding artificial noise to the image. NC, BER and SSIM of retrieved watermark is 1, 0 and 1 respectively, for all test images. This shows the proposed scheme is robust against this attack.

vii. **Salt and Pepper Noise:** This noise is added to the test images with noise density (D) from 0.01 to 0.10. NC and BER of retrieved watermark is above 0.9998 and below 0.0001 respectively, for all test images. SSIM of extracted watermark is 1 for all test images. This shows the proposed scheme is robust against this attack.

viii. **Speckle Noise:** This noise is added to all the test images with variance (V) from 0.01 to 0.10. NC and BER of retrieved watermark is above 0.9999 and below 0.00003 respectively, for all test

images. SSIM of extracted watermark is 1 for all test images. This shows the proposed scheme is robust against this attack.

ix. **Sharpening Attack:** The test images are sharpened with different combinations of radius (R) and amount (A). NC and BER of retrieved watermark is above 0.9999 and below 0.000091 respectively, for all test images. SSIM of extracted watermark is 1 for all test images. This shows the proposed scheme is robust against this attack.

x. **Sobel Attack:** This attack returns an image with the edges detected. NC and BER of retrieved watermark is above 0.9983 and below 0.0023 respectively, for all test images. SSIM of extracted watermark is above 0.9999 for all test images. This shows the proposed scheme is robust against this attack.

xi. **Blurring attack:** The images are blurred for different values of radius (R). NC and BER of retrieved watermark is above 0.9999 and below 0.00012 respectively, for all test images. SSIM of extracted watermark is 1 for all test images. This shows the proposed scheme is robust against this attack.

These results are presented in tables 5.1 and 5.2 from where it can be observed that performance of the proposed scheme is outstanding against all attacks on different images for various ranges. The values for NC in all the cases are above 0.99. BER values are close to 0 for all test images. This shows high robustness of the scheme.

Table 5.1: NC Results for different images against different attacks

	Airplane	Barbara	Girl	Goldhill	House	Lake	Lena	Mandrill	Peppers	Zelda
JPEG Compression	1	1	1	1	1	0.99	1	1	1	1
Rotation	0.9995	0.9993	0.9995	0.9988	0.9994	0.9995	0.9995	0.9994	0.9994	0.9991
Median Filter	1	1	1	1	1	1	1	1	1	1
Cropping	0.9999	0.9999	1	0.9992	1	1	0.9999	0.9999	1	0.9999
Gaussian Noise	1	1	1	1	1	1	1	1	1	0.9993
Poisson Noise	1	1	1	1	1	1	1	1	1	1
Salt and Pepper Noise	1	1	1	1	1	1	1	1	1	0.9999
Speckle Noise	1	1	1	1	1	1	1	1	1	1
Sharpening	1	1	1	1	1	1	1	1	1	1
Sobel	0.9983	0.9986	0.9977	0.9997	0.9988	0.9989	0.9983	0.9985	0.9985	0.9984
Blurring	1	0.99	1	1	1	1	1	1	1	0.99

Table 5.2: BER Results for different Images against different attacks

	Airplane	Barbara	Girl	Goldhill	House	Lake	Lena	Mandrill	Peppers	Zelda
JPEG Compression	0	0	0	0	0	0.00016	0	0	0	0
Rotation										
Rotation	0.00054	0.00067	0.00053	0.0011	0.00068	0.00064	0.00051	0.0007	0.00059	0.00091
Median Filter	0	0	0	0.000015	0	0.000091	0	0.000015	0	0.000015
Cropping	0.00006	0.000061	0.00003	0.000045	0.000045	0.00015	0.000061	0.000076	0.000045	0.00009
Gaussian Noise	0.000015	0.000045	0	0.00018	0.000015	0.000091	0.000015	0.00003	0	0.00025
Poisson Noise	0	0	0	0	0	0.00009	0	0	0	0.000015
Salt and Pepper Noise	0.000015	0.000015	0	0.000045	0.000015	0.000091	0.000015	0.00003	0	0.0001
Speckle Noise	0.000015	0	0	0	0	0.000091	0.000015	0	0	0.000015
Sharpening	0.000015	0	0	0	0	0.000091	0	0.000015	0	0.000015
Sobel	0.0017	0.0014	0.0023	0.0003	0.0012	0.0011	0.0017	0.0012	0.0008	0.00016
Blurring	0.000015	0.000015	0	0	0	0.000091	0.000015	0.000015	0	0.000015

Comparison of the proposed scheme with some recent color image watermarking schemes on different images against different attacks is shown in Table 5.3. The table clearly shows the superiority of the proposed scheme to the existing schemes in terms of NC and BER. Both the parameters have been separated by '/' and represented as NC / BER.

Table 5.3: Comparison of Proposed Scheme with Existing Color Image Watermarking Schemes

		Shao et al. (2016)	Roy and Pal (2017)	Xia et al. (2019)	Abraham and Paul (2019)	Fares et al. (2020)	Al-Otum (2020)	Proposed Scheme
		NC / BER	NC / BER	NC / BER	NC / BER	NC / BER	NC / BER	NC / BER
JPEG Compression	Q=30	- / 0.0015	-	- / 0.0054	0.8199 / 0.2422	-	0.994 / -	1 / 0.00016
	Q=40	-	0.9718 / 0.0352	-	0.8549 / 0.1982	0.97752 / -		1 / 0.00016
	Q=50	-	1.00 / 0.00	-	0.8873 / 0.1543	-	0.983 / -	1 / 0.00016
	Q=60	- / 0.0007	1.00 / 0.00	-	0.8057 / 0.2617	-	-	1 / 0.00016
	Q=70	-	1.00 / 0.00	- / 0.0036	0.8314 / 0.2295	-	-	1 / 0.00016
	Q=90	- / 0	-	-	-	-	-	1 /0.00016
Rotation	A=5	-	0.9698 / 0.041	- / 0.0037	-	-	-	0.9999 / 0.00021
	A=30	- / 0.0294	-	-	-	-	-	0.9997 / 0.00053
	A=35	-	-	-	-	0.93057 / -	-	0.9998 / 0.00055
	A=45	-	-	- / 0.0042	-	-	-	0.9998 / 0.00056
Median Filtering	$ws = 2 \times 2$	- / 0.0011	0.9973 / -	-	-	-	-	1 / 0
	$ws = 3 \times 3$	-	0.995 / -	- / 0.0098	-	0.8821 / -	0.995 / -	1 / 0
	$ws = 5 \times 5$	-	-	-	-	-	0.995 / -	1 / 0
Cropping	32×32	- / 0.0034	-	- / 0	-	-	0.9 / -	1 / 0.000015
	64×64	-	0.9879 / 0.1	- / 0	-	-	0.882 / -	0.9999 / 0.000061
	128×128	-	0.9652 / 0.0317	-	0.7500 / 0.2500	-	-	0.9999 / 0.00022

	256 × 256	-	0.8845 / 0.01392	-	0.5 / 0.5	-	-	0.9998 / 0.0008
Gaussian Noise	V=0.01	-	0.8967 / 0.1214	- / 0.02	-	0.90833 / -	-	1 / 0
	V=0.03	-	1 / -	-	-	-	-	1 / 0.000015
	V=0.05	- / 0.0042	-	-	-	-	-	1 / 0.00003
	V=0.15	- / 0.0103	-	-	-	-	-	1 / 0.000045
	V=0.25	- / 0.0134	-	-	-	-	-	1 / 0.000076
Sharpening	R=2, A=0.1	-	-	-	-	-	0.992 / -	1 / 0
Salt and Pepper Noise		- / 0.0031	0.8977 / 0.1201	- / 0.026	0.9710 / 0.0391	0.6437 / -	-	1 / 0.000015
Speckle Noise	V=0.001	-	0.9655 / 0.0408	-	0.9129 / 0.1211	-	-	1 / 0
	V=0.005	-	0.8838 / 0.1277	-	-	-	-	1 / 0

The '-' in various cells of the table refers that the readings for those cells is not given in the referred works.

It can be observed from table 5.3, in existing schemes NC for different images against *JPEG* Compression attack ranges from 0.8 to 0.99, while it is 1 for the proposed scheme. For Rotation, it ranges from 0.93 to 0.966 in the existing schemes, while for the proposed scheme it remains 0.99. For median filtering, it ranges from 0.88 to 0.99 for existing schemes and is 1 for the proposed scheme. For Cropping and Gaussian Noise, it ranges from 0.5 to 0.9 in the existing schemes, while for the proposed scheme it ranges between 0.99 and 1. For Sharpening, Al-Otum (2020) shows 0.992 that has been improved to 1 for the proposed scheme. For salt and pepper noise, it ranges from 0.64 to 0.97 and is 1 for the proposed scheme. BER values have also been enhanced remarkably. In the proposed scheme, BER tends towards 0. This robustness of the proposed scheme is ensured as non fine scale layer of the Curvelet coefficient matrices are used in constructing shares and the fine scale layer has been excluded as it just contains image edges and other details.

5.4.2 Time Complexity

As illustrated in Section 5.3, the primary time-consuming operations in the first phase of the proposed scheme are: DCuT, MS Construction and OS Construction. The 2D-DCuT has complexity $O(n^2 \log n)$ Candès and Donoho (2004), where n denotes the size of host image. The time-costing of MS and OS Construction usually involve binary operations on all pixels, hence their complexity can be accounted to $O(n)$. Thus, the time complexity of first phase is $O(n^2 \log n) + O(n)$. As, the second phase includes construction of MS and superimposition of MS and OS, its time complexity

is $O(n^2 \log n) + O(n)$.

Therefore, the total time complexity of the proposed scheme is $O(n^2 \log n) + O(n)$, which can be simplified to $O(n^2 \log n)$. Thus, it can be concluded that the time complexity of the proposed scheme mainly depends on DCuT.

5.4.3 Statistical Analysis

Given an image under test and a watermark, and assuming that the transmitted image has not suffered any attacks or unintentional distortions, the watermark detection test can be formulated as the binary hypothesis test

$$H_1 : o = f(w_1, w_2, x, c), H_0 : o = c \tag{5.5}$$

where o represent OS that is constructed using a binary cover image c, a watermark WI provided by user and a self constructed watermark W_2 that is constructed from the transmitted host image x. The goal of the watermark detection testis to decide whether the share o has been constructed using w_2. Let $S \in H_1, H_0$ be the decision made in watermark detection test. The probability of false positives can be defined as:

$$P_{FP} = Pr((OR(m, o) == W)|H_0) \quad \ldots (5.6)$$

i.e. P_{FP} calculates the probability (Pr) of retrieving the watermark w by superimposing m and o using OR operation, given hypothesis H_0 is true. The requirement of the scheme lies to minimize this probability, to ensure reliability. The probability of true detection can be defined as:

$$P_{TP} = Pr((OR(m, o) == W)|H_1) \quad \ldots (5.7)$$

i.e. P_{TP} calculates the probability (Pr) of retrieving the watermark w by superimposing m and o, given hypothesis H_1 is true. The requirement of the scheme lies to maximize this probability, to ensure effectiveness. To prove the above hypothesis, a test was conducted on 228 color images to test the false positive and true detection cases. The results are shown in Table 5.4.

Table 5.4: Statistical Analysis of Proposed Scheme

Images	Count	TP	FP

General Images	30	30	0
Aerial Images	37	37	0
Marbel Images	27	27	0
Miscellaneous Images	134	134	0
Total	228	228	0

It can be observed from Table 5.4 that when different types of images were tested, the count for false positives (FP) remained minimum while the count for true positives (TP) remain maximum.

5.5 Conclusion of the Chapter

In this Chapter, a secure and robust copyright protection scheme for color images is proposed. The non fine scale layers of curvelet transform coefficients of Y channel of the image have been utilized to provide high robustness to the scheme. An additional watermark is created from C_b, C_r channels of the image to handle the false positive cases. To prove the copyright, the watermarks can be retrieved by OR-superimposition of OS with MS and its rotated version. Experimental results have been performed on different images for different attacks. NC value of the extracted watermark is maintained at 0.99 or more while BER is maintained below 0.1, which shows that the scheme has outstanding resistance to attacks. The advantages of the proposed copyright protection scheme are that the watermark's size is not restricted to the size of the protected image; the self constructed watermark handles false positive cases, and meaningful shares ensure security of the scheme. Comparison with the other exiting copyright protection schemes for color images reveals that the proposed scheme gives better performance.

CHAPTER 6

Robust Copyright Protection Scheme for Multiple Images and Owners using LBP-SURF Descriptors

.

6.1 Introduction

The existing copyright protection schemes Amiri and Moghaddam (2016); Liu and Wu (2011) for multiple images create noisy shares that are distributed to the owners and create a suspicion of some secret data being shared. Also, these schemes have a restriction that every owner has to present its share prove the copyright, else it can not be verified. To address these concerns, an EVCS based copyright protection scheme is proposed that works for multiple images with multiple owners. This scheme creates meaningful noiseless OSs for the owners and their copyright is proved

Contents of the work presented in this Chapter have been published in *The Visual Computer*, https://doi.org/10.1007/s00371-020-01883-9, 2020. (SCI Indexed)

by superimposing qualified set of OSs. Here, three types of shares are created, *i.e.* MS, OS and key share. The combination of LBP and SURF in the proposed scheme makes it robust against different image processing attacks especially the rotation attack. The watermark size is unrestricted, as SURF is flexible to select any number of feature points to create the shares corresponding to watermark. Use of LBP ensures no false positive cases. Every OS is created using MS and the watermark. The OS is further used to create key share and is stored with the TA. When the copyright of multiple images needs to be verified, the OSs and key share are superimposed on each other to retrieve the watermark. The experiments have been performed to show that the scheme verifies the copyright of digital images efficiently, and is robust and imperceptible. Comparisons with the existing copyright protection schemes show better performance of the proposed scheme.

6.2 Preliminaries

In this section, SURF, LBP and K-means clustering are discussed.

6.2.1 Speeded Up Robust Features

In images, feature refers to a piece of information which represents the image like points, edges, objects, neighborhood, *etc.*. SURF, inspired by the SIFT descriptor, is a local feature detector and descriptor. Authors claim Bay et al. (2008) that SURF has higher calculation speed than SIFT without causing loss of performance. Also, SURF is more robust than SIFT against different transformations, like scaling, rotation, image blur, lighting changes and JPEG compression, among others.

SURF uses Gaussian scale analysis and is faster as it uses integral images. SURF determines points of interest by using blob detector based on determinant of Hessian matrix. The Hessian matrix H at point $X = (x, y)$ at scale σ is represented as follows:

$$H(X,\sigma) = \begin{bmatrix} L_{xx}(x,\sigma) & L_{xy}(x,\sigma) \\ L_{xy}(x,\sigma) & L_{yy}(x,\sigma) \end{bmatrix} \quad \ldots (6.1)$$

where $L_{xx}(x,\sigma)$ is the convolution of Gaussian second order derivative of image I at point x, and similarly for $L_{xy}(x,\sigma)$, $L_{yy}(x,\sigma)$ and $L_{yx}(x,\sigma)$. The box filter of size 9×9 is an approximation of a Gaussian with $\sigma = 1.2$ and represents the lowest level for blob-response maps. SURF constructs a feature descriptor of 64 bits using neighborhood around the key points and haar wavelet responses

for these regions. To handle larger viewpoint changes, the feature descriptor can be extended to 128 bits. SURF features are invariant to rotation and scaling.

6.2.2 Local Binary Pattern

LBP is a simple and efficient texture descriptor proposed by Ojala et al. (1996). It generates a binary label for pixels of an image from their neighborhood. Every pixel is compared with its eight surrounding neighbors; the neighbors having smaller pixel value than the central pixel are assigned 0 while the equal or greater pixels are assigned 1. Binary value is obtained by concatenating these eight bit values in clockwise direction starting from top left neighbor. The equivalent decimal value for this binary value replaces the central pixel. Histogram of these code frequencies is constructed over a region and is used as texture descriptor. LBP(P,R) generates 2^P different binary codes, formed by P neighboring pixels with radius R. An example for LBP(8,1) is shown in Figure 6.1. The value of LBP code of a pixel *(x,y)* is given by:

$$LBP(P,R) = \sum_{p=0}^{P-1} f(val_p - val_c)2^p \qquad \ldots(6.2)$$

where, val_p refer to neighboring pixel values and val_c refer to the center pixel value at *(x,y)* and f is defined as:

$$f(x) = \begin{cases} 1, & if\, x \geq 0 \\ 0, & if\, x < 0 \end{cases} \qquad \ldots(6.3)$$

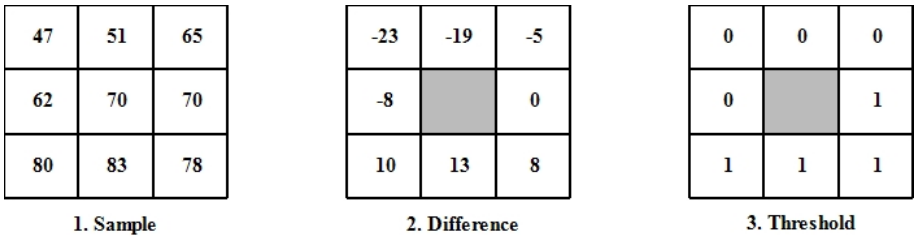


Figure 6.1: An LBP example for P=8, R=1

6.3 Proposed Scheme

The proposed copyright protection scheme is discussed in this section. The scheme is performed in two phases: Shares Construction and Ownership Verification, which are explained in Figure 6.2.

6.3.1 Shares Construction

This phase is further performed in to steps: MS Construction and OS Construction. Firstly, t host images $H_1, H_2, H_3, ...H_t$ are used to construct MS by utilizing SURF, LBP and K-means clustering. The steps for MS construction are described in Algorithm 6.1. LBP and SURF extracts textual information and features around robust key-points, respectively from the image. These features collectively form a Master Vector which is then reshaped to form *MM*. This *MM* is divided into blocks such that the number of blocks are equal to the number of watermark bits. The blocks obtained are categorized into 2 clusters using K-means clustering to form a binary share considered as MS.

Algorithm 6.1 MS Construction

Input: t Host Images $HI_1, HI_2, HI_3, ...HI_t$, WI of size $h_w \times w_w$
Output: MS

1: Initialize a Null Master Vector
$MV = [\,]$
2: **for** i = 1 to t **do**
Extract LBP features from HI_i and store as FV_{LBP} of length l_l.
$FV_{LBP} = \{L_i \mid i = 1, 2, ...l_l\}$
Apply SURF operator on HI_i to obtain s strongest robust key-points, where s is:
$s = \dfrac{\frac{h_w \times w_w}{t} - l_s}{l_l}$,
where l_s represents length of FV_{SURF}
Extract features for the obtained s key-points,
$FV_{SURF} = \{S_i \mid i = 1, 2, ...l_s\}$
Concatenate FV_{LBP} and FV_{SURF} to MV.
3: Reshape MV to form a *2D-MM* of size $h_{mm} \times w_{mm}$
where $h_{mm} = w_{mm} = \sqrt{l_{mv}}$, l_{mv} represents length of MV
4: Divide MM into m non overlapping blocks blk_{ij} of size $h_b \times w_b$,
$B = \{blk_{ij} \mid 1 \le i \le h_w, 1 \le j \le w_w\}$,
$m = h_w \times w_w, h_b = \frac{h_{mm}}{h_w}, w_b = \frac{w_{mm}}{w_w}$
5: Classify blocks into 2 clusters using k-means clustering to form M of size $h_m \times w_m$,
where $h_m = h_w$ and $w_m = w_w$.

The steps to create a noisy OS using MS and *WI* is described in Algorithm 6.2 with an example in Figure 6.3.

n binary images are distributed among the owners which are referred as their ownership images

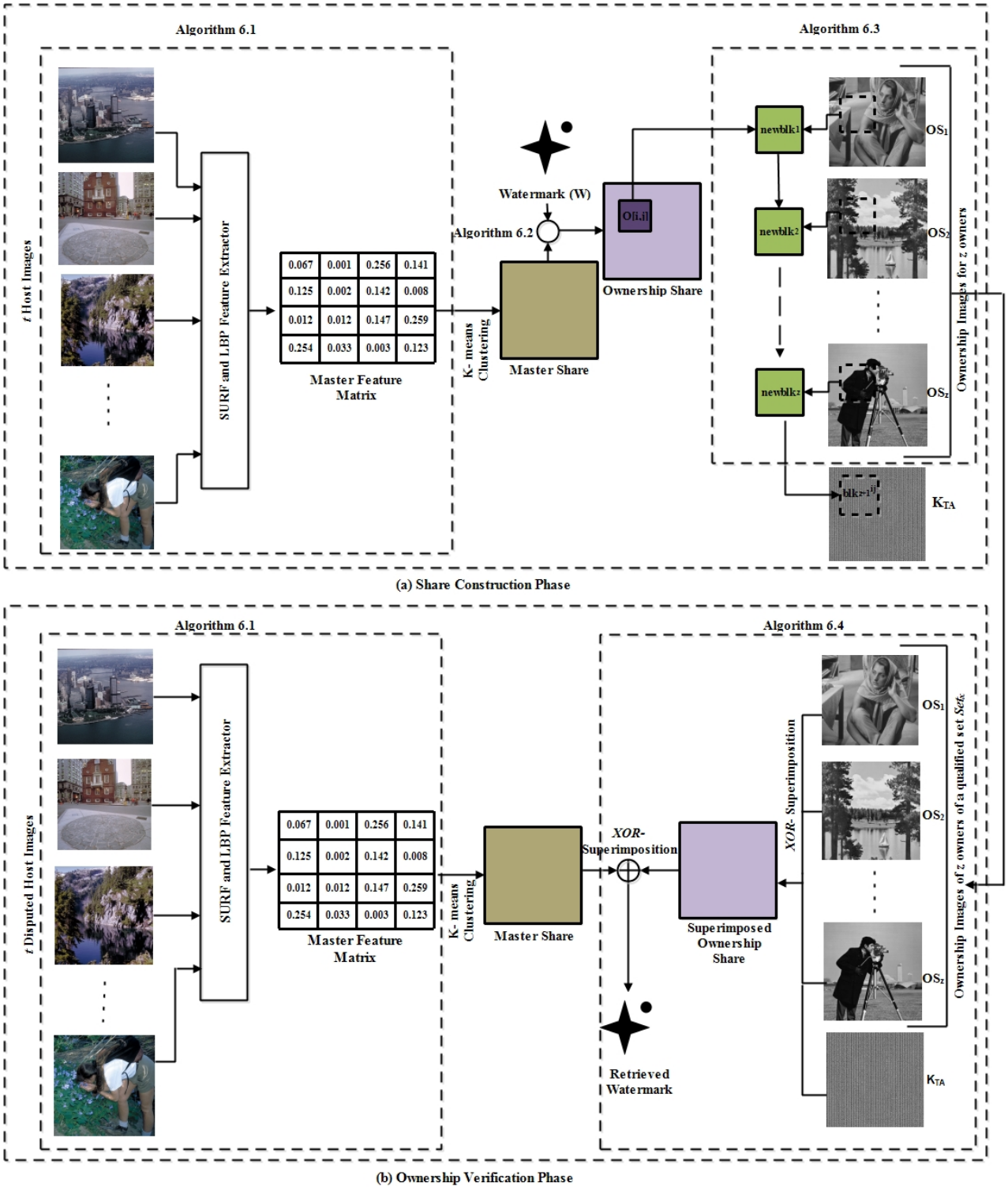


Figure 6.2: Block Diagram of the Proposed Scheme

Algorithm 6.2 Meaningless OS Construction

Input: MS and Watermark Image (WI) of size $h_w \times w_w$
Output: Meaningless OS of size $h_w \times w_w$

1: **for** i = 1 to h_w **do**
2: **for** j = 1 to w_w **do**
3: **if** $WI(i, j) == 0$ **then**
$OS(i, j) = MS(i, j)$
4: **else**
$OS(i, j) = Complement(MS(i, j))$

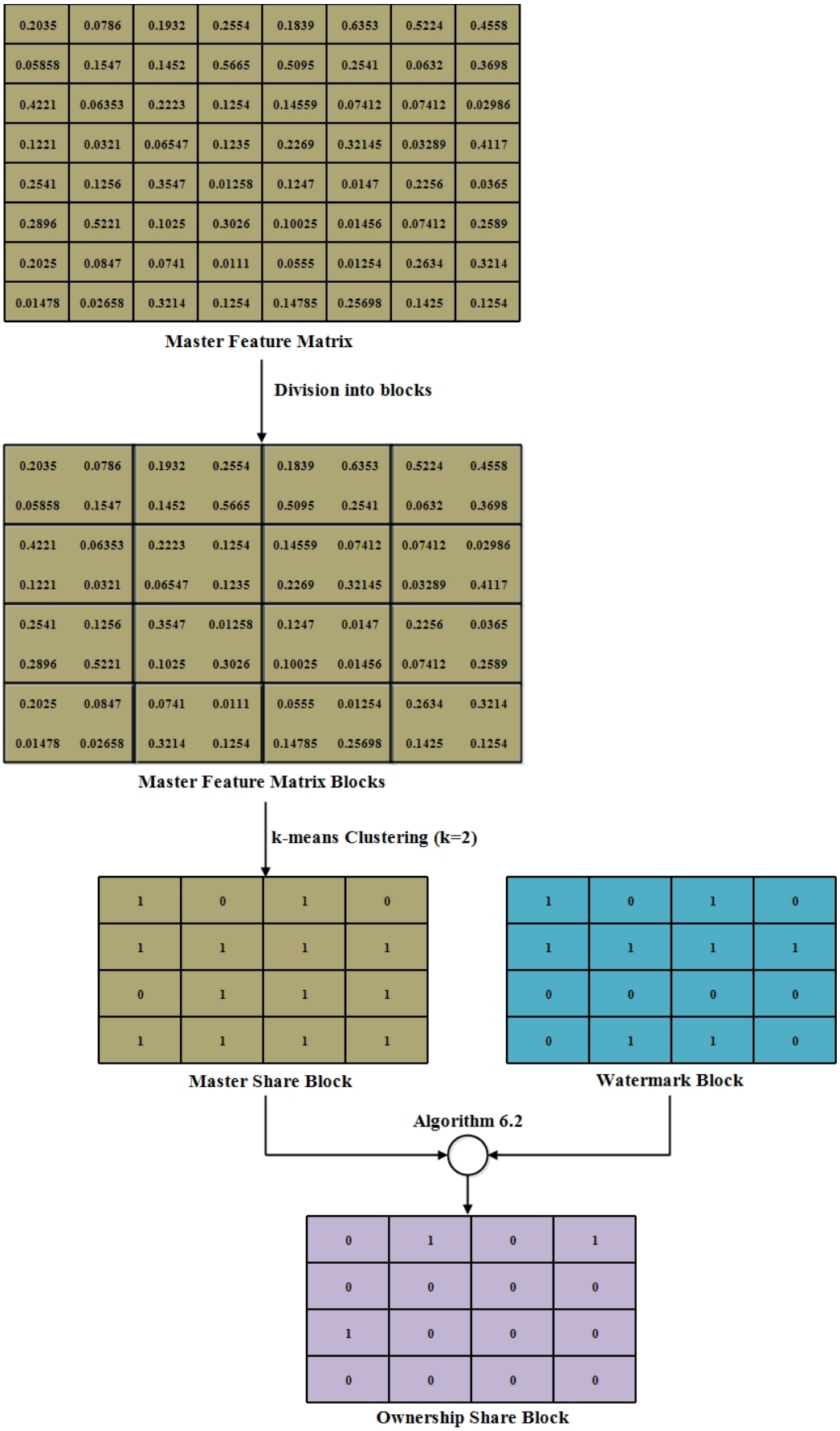


Figure 6.3: An Example of creating MS and OS from MM

$O_1, O_2, O_3, ...O_n$. These ownership images along with constructed noisy OS are used to create a Key Share K_{TA} using Algorithm 6.3 which is stored with TA.

Let the collection of owners is denoted as $(\tau_{qual}, \tau_{forb})$, where τ_{qual} is a set of qualified sets of owners who have the authority to retrieve the watermark for copyright verification while τ_{forb} is the set of forbidden owners. Let N be a set of n ownership images such that $P(N)$ denotes power set of N, *i.e.* set of all subsets of N. During the verification phase, OS is regenerated by superimposing K_{TA} and ownership images of any qualified subset $Set_x \in \tau_{qual}$ where $\tau_{qual} = Set_1, Set_2, ..., Set_q$ and $Set_x = O_1, O_2, ..., O_z$, $1 \leq x \leq q$. If owners from any forbidden set τ_{forb} where τ_{forb} = P(N) - $Set_1, Set_2, ..., Set_q$, superimpose their images with K_{TA}, any information about OS cannot be retrieved. The procedure to construct meaningful OS is described in Algorithm 6.3 with an example in Figure 6.4, that explains construction of a block in K_{TA} using blocks of $O_1, O_2, O_3, ...O_z$ and OS pixel.

A qualified set of owners is randomly chosen from τ_{qual} that is used to construct K_{TA}. The ownership images $O_1, O_2, ..., O_z$ are divided into equal sized blocks. The number of blocks created should be equal to the number of bits in OS. In the verification stage, when constructed K_{TA} is superimposed with the ownership images of owners from qualified set, OS is retrieved back. This procedure is described in Algorithm 6.3.

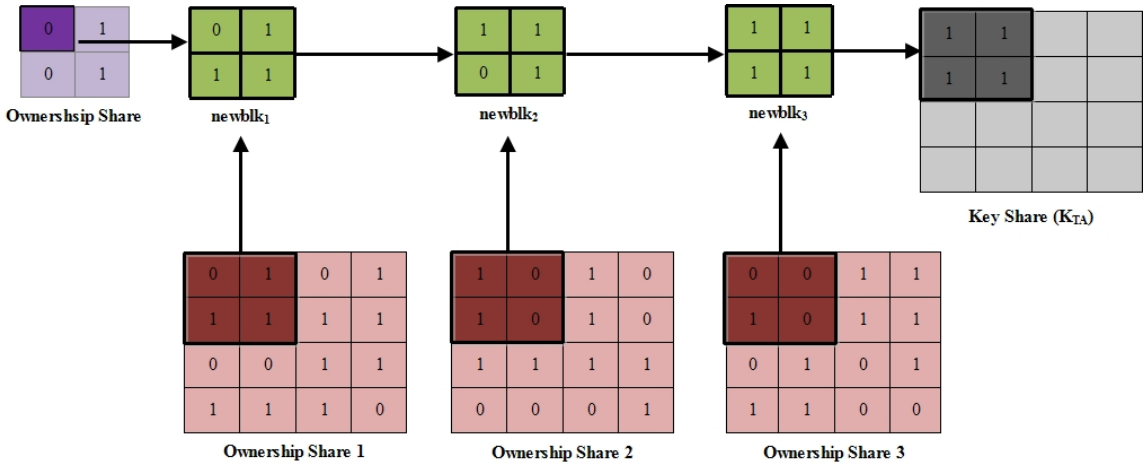


Figure 6.4: An Example to create a block in K_{TA} from a pixel in O using Algorithm 6.3

The MS size is dependent on size of feature vector obtained from host image. The size of feature vector depends on parameter s that is described in the Algorithm 6.1. The watermark size should be equal to the MS size that further depends on value of s. Thus, value of s can be decided in accordance with watermark size and vice versa. The size of OS is dependent on the size of MS and watermark.

Algorithm 6.3 Key Share Construction

Input: OS of size $h_w \times w_w$, Ownership Images $OS_1, OS_2, OS_3, ...OS_n$ of size $h_o \times w_o$, General access structure (τ_{qual},τ_{forb}), where τ_{qual} = {Set_1,Set_2,.....Set_q} and τ_{forb} = P(N) - {Set_1,Set_2,.....Set_q}.

Output: Key Share K_{TA} of size $h_o \times w_o$

Divide all ownership images $OS_1, OS_2, OS_3, ...OS_n$ into non overlapping blocks of size $h_{ob} \times w_{ob}$,
$OBlks_y = \{blk_y^{u,v} \mid y = 1,2,.....n; 1 \le u \le h_w; 1 \le v \le w_w\}$
where $h_{ob} = \frac{h_o}{h_w}$, $w_{ob} = \frac{w_o}{w_w}$
Select a random set Set_x of length z from τ_{qual}.
for i = 1 to h_w **do**
  for j = 1 to w_w **do**
    if $OS[i,j] == 0$ **then**
      $newblk_1 = blk_1^{i,j}$
    else
      $newblk_1 = Complement(blk_1^{i,j})$
    if $z \ge 2$ **then**
      for g= 2 to z **do**
        $newblk_g$ = CreateNewBlock($newblk_{g-1}$,$blk_g^{i,j}$)
      $blk_{z+1}^{i,j} = newblk_z$
  $K_{TA}[i,j] = blk_{z+1}$
function CREATENEWBLOCK(U,V)
  for e = 1 to h_{ob} **do**
    for f = 1 to w_{ob} **do**
      if $U[e,f] == 0$ **then**
        $V[e,f] = U[e,f]$
      else
        $V[e,f] = Complement(U[e,f])$
  return

6.3.2 Ownership Verification

To prove the ownership of a set of images, a master share MS' is constructed from these images, using Algorithm 6.1. The set Set_x with z owners chosen randomly from τ_{qual} in Algorithm 6.3 is used to prove the copyright. The key share K_{TA} stored with TA is superimposed with ownership images of z owners belonging to Set_x using XOR-operation, that results in O''. This O'' is further reduced to O' by discarding the extra pixels. The constructed O' and M' are superimposed to retrieve watermark W'. If W' is similar to the owners' watermark, their ownership is verified.

Algorithm 6.4 Ownership Verification

Input: Ownership Shares $OS = \{OS_i \mid 1 \leq i \leq z\}$ of size $h_o \times w_o$, where z = number of owners in qualified set Set_x

Output: Watermark W' of size $h_w \times w_w$

1: Create MS' from disputed Host Images using Algorithm 1
2: Retrieve K_{TA} from TA
3: $OS'' = K_{TA} \oplus OS_z$
4: **for** k = z-1 to 1 **do**
$OS'' = OS'' \oplus OS_k$
5: Divide OS'' into blocks of size $h_{ob} \times w_{ob}$
$OBlks = \{blk^{u,v} \mid 1 \leq u \leq h_w; 1 \leq v \leq w_w\}$
6: **for** i = 1 to h_w **do**
7: **for** j = 1 to w_w **do**
8: **if** All bits of blk^{ij} are equal to 1 **then**
$OS'[i, j] = 1$
9: **else**
$OS'[i, j] = 0$
10: $W' = M' \oplus OS'$
11: If WI' is similar to WI, copyright can be proved.

6.3.3 Significance of SURF and LBP in the Proposed Scheme

SURF is a patented local feature detector and descriptor, partly inspired by the SIFT descriptor. As claimed by Bay et al. (2008), SURF presents two main improvements in comparison to SIFT: firstly, higher speed of calculation without causing loss of performance and secondly, smaller size feature vector. SURF is only half of the size of the SIFT descriptor. SIFT returns a feature vector of 128-dimension while SURF returns a feature vector of 64-dimension for an image of size 512 × 512. Also, SURF displays high robustness against different types of geometric and photometric transformations, such as scaling, rotation, image blur, lighting changes and JPEG compression *etc.* The Haar wavelets used in SURF extraction for the orientation assignment around the keypoints,

enhances the robustness and minimizes the computational cost. A reproducible orientation for the interest point is identified, that makes SURF invariant to the rotation angles proportional to 90° Karami et al. (2017); Zhu et al. (2013). When the image is rotated by other angle, the Haar Wavelet coefficients get modified leading to the different direction and description vector of the feature point Zhu et al. (2013). Thus, the original and rotated image generate different MSs, making the scheme fragile against rotation attack.

LBP is a simple and efficient global texture descriptor proposed by Ojala et al. (1996). LBP calculates local representation of image texture and returns a global feature vector of the image. This local representation is performed by comparing each pixel with its surrounding neighborhood of pixel values. LBPs are used to characterize the texture and pattern of an image/object in an image. They process pixels locally which leads to a more robust, powerful texture descriptor. This characteristic of LBP operator can be utilized in developing watermarking schemes that need an effective representation of local structure information of the image.

SURF and LBP together help in making the scheme highly robust against rotation for all the angles Jiang et al. (2015); Prabhakar and Kumar (2012). A combination of SURF and LBP has been used in the proposed scheme to create a robust MS that efficiently represents the host image. LBP returns a robust global feature of the image that helps in ensuring zero false positive cases and high robustness against rotation. SURF helps in representing the local features of the image around selected robust keypoints. The local SURF feature vectors help in ensuring high robustness against various geometric attacks. The flexibility in the number of chosen keypoints allows the flexibility in the watermark size.

If the MS is constructed using only LBP feature vector, its size would be restricted to just 59-dimension and would not be robust against different geometric attacks except rotation. If the MS is constructed just with only SURF features, in some cases, the MS constructed from other images can also retrieve the watermark. Thus resulting in false positive cases. Also, the scheme would not perform well against rotation attack for all angles. This scenario has been represented in the Figure 6.5.

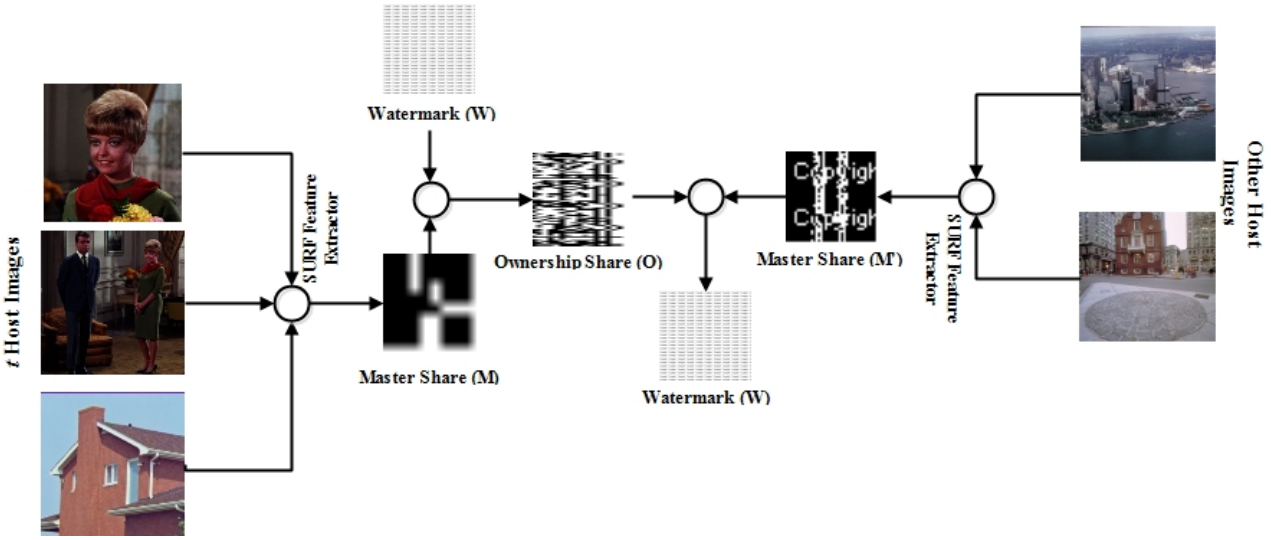


Figure 6.5: A Scenario where only SURF is used for MS Construction

6.4 Experimental Results and Discussion

The proposed scheme is experimented using MATLAB (R2019a), on 64-bit Windows 10, Intel(R) Core(TM) i5-6200 CPU @2.30GHz 2.40 GHz Processor, 8.00 GB RAM. 300 different *8*-bit host images of size 512×512 are tested with binary watermark of size 64×64 using the above setup. Three simulations are performed to test the effectiveness of the proposed scheme:

i. Simulation 1: One host image and one owner

ii. Simulation 2: Two host images and two owners

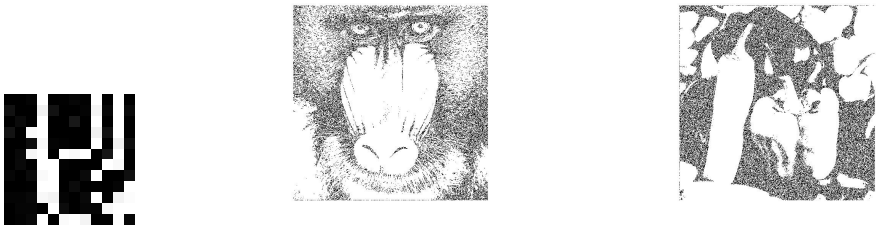
iii. Simulation 3: Thirty host images and ten owners

Host images, watermark and cover images used for simulation 2 are shown in Figure 6.6 and the resulting OSs are shown in Figure 6.7 respectively.

Similarity measurements like Normalized Correlation NC, Tamper Assessment Function TAF and Bit Error Rate BER are used to evaluate the performance of the scheme.

(a) (b) (c) (d) (e)

Figure 6.6: Test Host Images, Watermark and Cover Images (a) Host Image 1 (b) Host Image 2 (c) Watermark (d) Cover Image 1 (e) Cover Image 2



(a) (b) (c)

Figure 6.7: Shares Generated (a) OS (b) OS_1 (c) OS_2

When the images are transmitted, they can be manipulated unethically by the unauthorized users. Hence, the proposed scheme is experimented with various image manipulation attacks and the robustness results are shown in Figures 6.8-6.16 with the help of parameters NC, TAF and BER. According to Voloshynovskiy et al. (2001), Stirmark benchmark is a watermarking benchmark which divides image processing attacks into different categories like rotation, scaling, enhancement, etc. Kutter and Petitcolas (1999) divided these attacks into sections like geometric, noise addition, enhancement, compression and combined attacks, based on their properties. These classification is as follows:

i. **Geometric Transformation Attacks:** The image is transformed using rotation, resizing and cropping and then the robustness is the results are shown in Figures 6.8, 6.9 and 6.10 for *NC*, *BER* and *TAF*.

   - **Rotation Attack:** Here, the test images have been rotated with different angles (A) ranging from 10°to 60°. The results in Figure 6.8 show that for all degrees of rotation for different simulations, the valuse of NC and TAF is above 0.8 while BER is always below 0.1, ensuring high robustness against rotation attack.

   - **Cropping Attack:** To focus on a specific part of the image, cropping is done for that part and rest of the image is neglected. Robustness of the proposed scheme is tested against cropping for different window sizes 16×16, 32×32, 64×64, 128×128, and 256×256. The results in Figure 6.9 show that NC and TAF are mostly above 0.9 and 0.8 respectively, while BER is below 0.1, ensuring high robustness against cropping attack.

   - **Resizing:** Images can be resized intentionally or unintentionally in uniform or non-uniform manner. The proposed scheme is tested against resizing to prove its robustness. The test images are resized for different values of scale factor F ranging from 0.5 to 5 and the results in Figure 6.10 prove high robustness of the scheme against resizing attack as

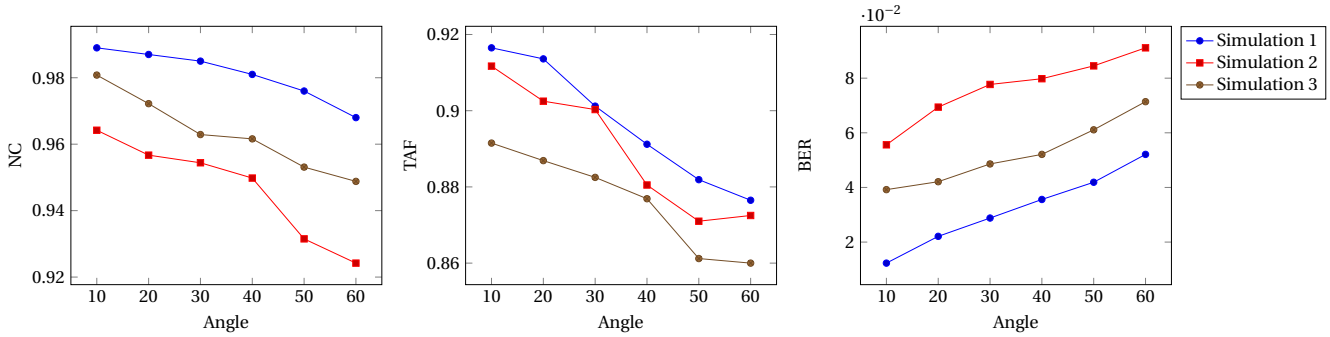


Figure 6.8: NC, TAF and BER values for Simulations 1,2 and 3 for different rotation angles

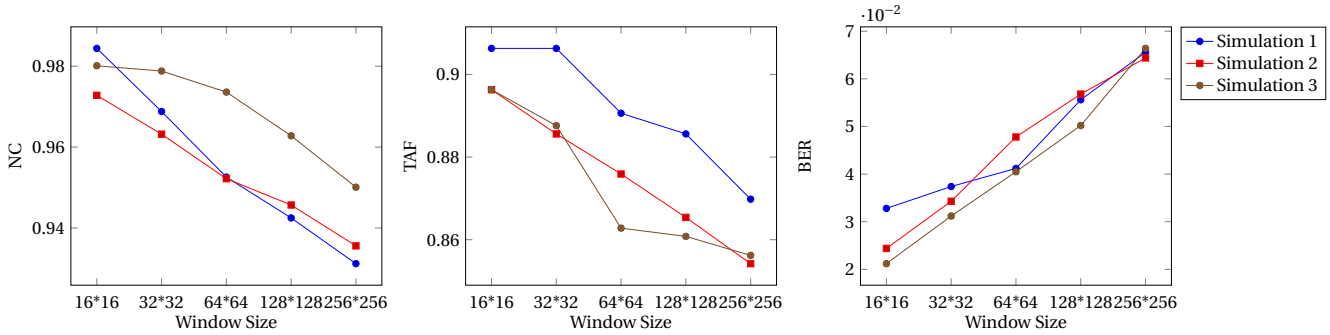


Figure 6.9: NC, TAF and BER values for Simulations 1,2 and 3 for different cropping window sizes

NC and TAF are mostly above 0.9 and 0.8 respectively, while BER is below 0.1.

ii. **Noise Addition Attack:** Apart from the geometrical attacks, other image processing attacks include noise addition attacks where additive noise and uncorrelated multiplicative noise is added to the images. The proposed scheme is tested against Gaussian, Poisson, Salt & Pepper, Speckle and Sobel. The results are shown in Figures 6.11, 6.12 and 6.13 for different simulations using NC, TAF and BER parameters.

- **Gaussian Noise Attack:** Gaussian noise is one of the most common statistical noise processing operations where the noise is varied by its variance with zero mean. To test the robustness of the proposed scheme, the gaussian noise is added to the test images with

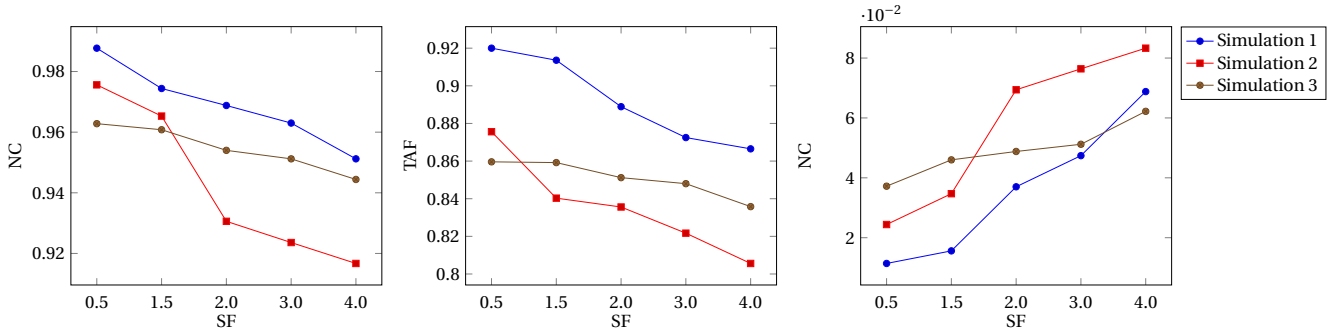


Figure 6.10: NC, TAF and BER values for Simulations 1,2 and 3 for different resizing factors

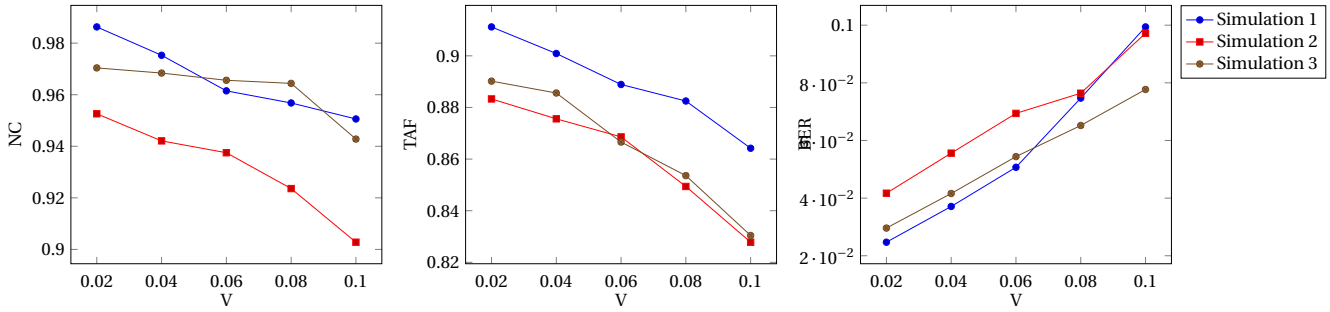


Figure 6.11: NC, TAF and BER values for Simulations 1,2 and 3 for Gaussian Attack with different values of variance V

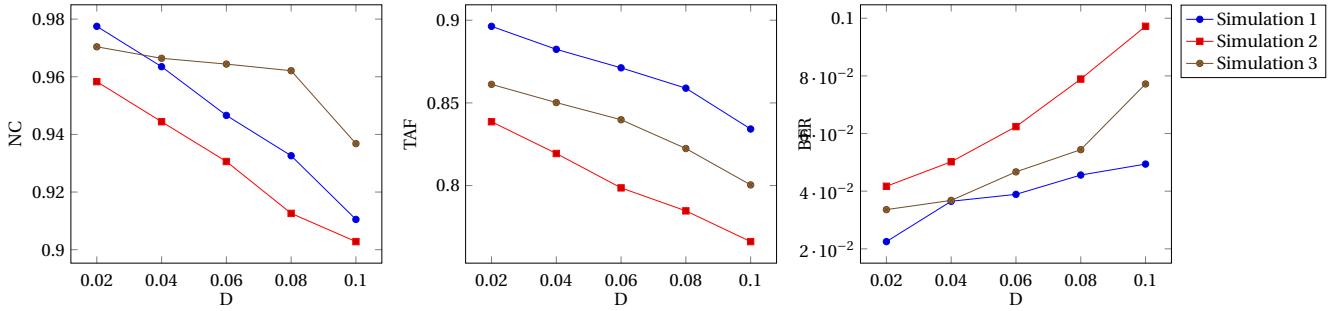


Figure 6.12: NC, TAF and BER values for Simulations 1,2 and 3 for Salt and Pepper Noise with different values of noise density D

mean 0 and variance (V) ranging from 0.01 to 0.09 and high values of NC and TAF while low value for BER ensure high robustness of the proposed scheme in every simulation.

- **Salt and Pepper Noise:** This noise occurs due to the error in the pixel value during the data transmission. This modified pixel is either set to zero or maximum value, giving a salt and pepper appearance to the image. The proposed scheme has been tested for robustness against this noise by adding it to the test images with noise density (D) ranging from 0.01 to 0.09. From the Figure 6.12 it can be observed that the proposed scheme shows high robustness against this noise, as NC and TAF are above 0.9 and 0.8 respectively while BER is below 0.1 for every simulation and at all densities.

- **Speckle Noise:** This is a multiplicative noise where speckle occurs inherently as granular noise. The variance of a pixel is equal to the variance of the local area centered around it. The robustness of the proposed scheme has been tested by adding this noise to all the test images with variance (V) ranging from 0.01 to 0.10 and the results in Figure 6.13 prove high robustness of the proposed scheme against this noise.

iii. **Enhancement Technique Attack:** Some of the common enhancement techniques like median filter and sharpening are applied to the test images to enhance their quality. To test the

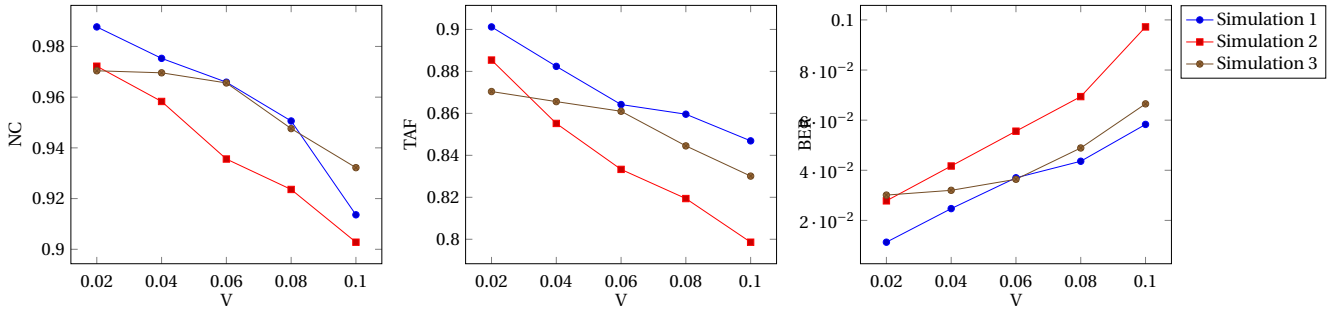


Figure 6.13: NC, TAF and BER values for Simulations 1,2 and 3 for Speckle Noise with different values of variance V

robustness of the proposed scheme, these attacks are applied to the host images and the results are shown in Figures 6.14 and 6.15.

- **Median Filtering:** A median filter is applied to an image to reduce the noise. The center pixel value of the window is replaced with the middle value of the sorted pixels. To test the robustness of the proposed scheme, the test images are applied filtering attack for window sizes (ws) of 2×2, 3×3, 4×4, 5×5, 6×6 and 7×7 and their results in Figure 6.14 ensure high robustness of the scheme.
- **Sharpening:** Sharpening attack is used to detect high frequency noise introduced by unauthorized users. The test images are sharpened with different combinations of radius (R) and amount (A). Seven cases have been taken for experimentation. Case C1, C2, C3 represent R=1.0, and A=0.2, 0.5, 0.8 respectively for the three cases. Case C4, C5, C6 and C7 represent R=2.0, A=1.1, 1.4, 1.7, 2.0 respectively for the four cases. It can be observed from Figure 6.15 that values of NC and TAF are usually maintained above 0.9 and 0.8 respectively, while BER is maintained below 0.1, which ensures high robustness of the proposed scheme against sharpening.

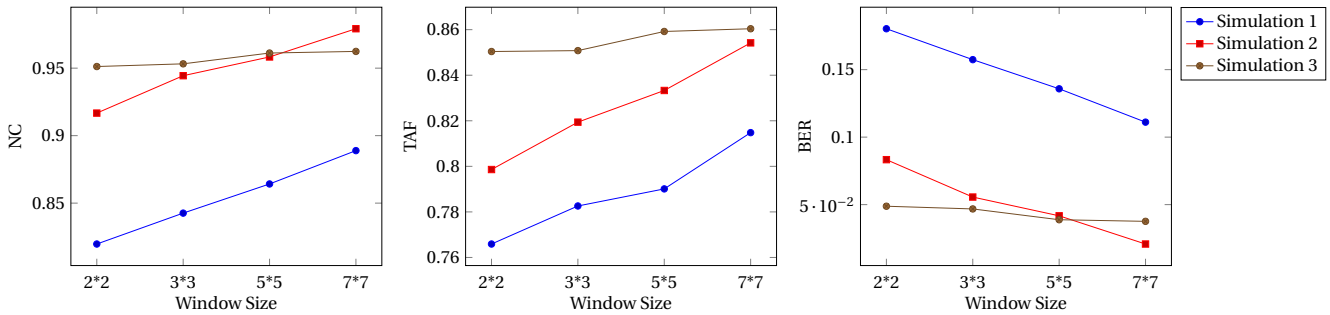


Figure 6.14: NC, TAF and BER values for Simulations 1,2 and 3 for Median Filtering Attack with different window sizes

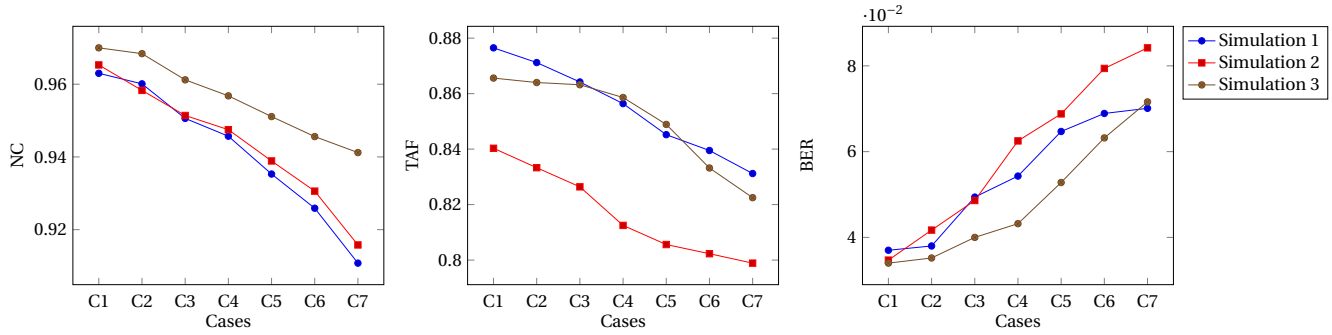


Figure 6.15: NC, TAF and BER values for Simulations 1,2 and 3 for Sharpening Attack for different combinations of R and A

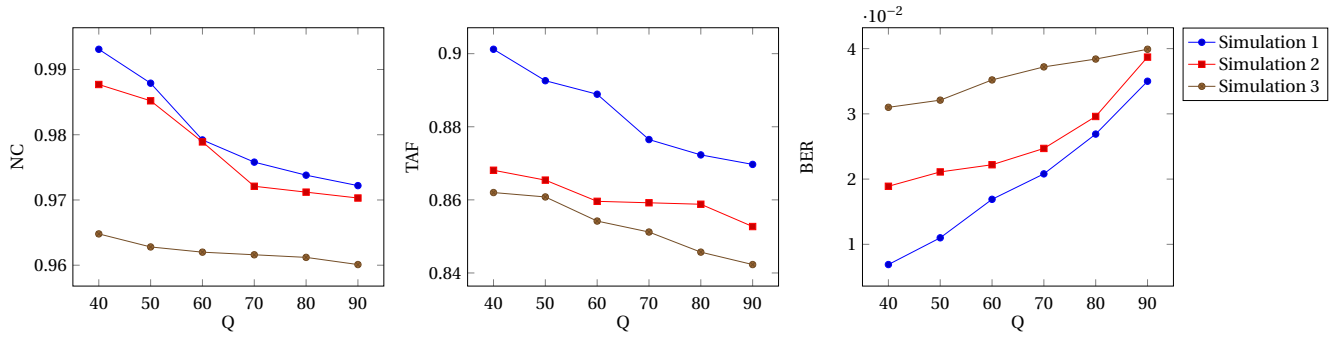


Figure 6.16: NC, TAF and BER values for Simulations 1,2 and 3 for different Compression Quality Q

iv. **Compression Attack:** The images are compressed and tested for robustness. The results for this attack are shown in Figure 6.16.

- ***JPEG* Compression:** *JPEG* Compression is one of the most widely used manipulation attack. The test images are compressed with quality (Q) factor ranging from 40 to 90. High values of NC and TAF, while low values of BER for the retrieved watermarks shown in Figure 6.16 ensure high robustness of the proposed scheme against *JPEG* compression. Even when 30 images had been compressed in Simulation 3, the NC and TAF values are still maintained above 0.9 while BER is maintained below 0.1, thereby ensuring high robustness.

v. **Combinational Attack**: To test the robustness of the scheme, some combinations of the above discussed attacks are applied on the test images and the results have been shown in Table 6.1. The results are shown for random combinations of two and three attacks on Simulation 1, 2 and 3. The results show that even when the image undergoes multiple attacks, the NC values are above 0.8 for almost every combination, thereby ensuring high robustness. Thus even in such cases, the watermark can be retrieved and used to prove the copyright.

Table 6.1: NC, TAF and BER values for Simulations 1, 2 and 3 for different combinational attacks

	Simulation 1			**Simulation 2**			**Simulation 3**		
	NC	**TAF**	**BER**	**NC**	**TAF**	**BER**	**NC**	**TAF**	**BER**
Noise Addition + Geometric Transformation									
Gaussian + Resize	0.963	0.8765	0.037	0.9608	0.858	0.0392	0.9306	0.8125	0.0694
Gaussian + Rotate	0.9444	0.8264	0.0556	0.9383	0.8519	0.0617	0.9375	0.8125	0.0625
Poison + Rotate	0.9383	0.8519	0.0617	0.9236	0.7986	0.0764	0.9196	0.8192	0.0804
Geometric Transformation + Enhancement									
Sharpen + Rotate	0.9753	0.8889	0.0247	0.9608	0.8592	0.0392	0.9306	0.8125	0.0694
Rotate + Sharpen	0.9522	0.8759	0.0478	0.9375	0.8125	0.0625	0.9167	0.7986	0.0833
Rotate + Median Filter	0.9444	0.8432	0.0556	0.9383	0.8519	0.0617	0.9306	0.8056	0.0694
Noise Addition + Compression									
Poisson + Compression	0.963	0.8765	0.037	0.9583	0.8333	0.0417	0.9552	0.852	0.0448
Gaussian + Compression	0.9522	0.8759	0.0478	0.9444	0.8194	0.0556	0.9306	0.8056	0.0694
Geometric Transformation + Compression									
Resize + Compression	0.9506	0.8642	0.0494	0.9514	0.8264	0.0486	0.9444	0.8432	0.0556
Rotate + Compression	0.9375	0.8125	0.0625	0.9306	0.8125	0.0694	0.9259	0.8395	0.0741
Rotate + Resize + Compression	0.9196	0.8192	0.0804	0.8958	0.7708	0.1042	0.8519	0.7778	0.1481
Noise Addition + Enhancement									
Gaussian + Sharpen	0.9259	0.8395	0.0741	0.9236	0.8056	0.0764	0.9196	0.8192	0.0804
Salt pepper + Sharpen	0.9753	0.8889	0.0247	0.9722	0.8472	0.0278	0.9676	0.8652	0.0324
Poisson + Salt pepper + Sharpen	0.9259	0.8395	0.0741	0.9444	0.8194	0.0556	0.8148	0.7407	0.1852
Enhancement + Compression									
Median Filter + Compression	0.9506	0.8642	0.0494	0.9583	0.8333	0.0417	0.9512	0.848	0.0488
Multiple Noises									
Poisson + Sobel	0.9375	0.8125	0.0625	0.9306	0.8125	0.0694	0.9236	0.7986	0.0764
Poisson + Salt pepper	0.963	0.8765	0.037	0.9636	0.8612	0.0364	0.9628	0.8596	0.0372
Poisson + Speckle	0.9506	0.8642	0.0494	0.9722	0.8472	0.0278	0.954	0.8512	0.046
Sobel + Speckle	0.9753	0.8889	0.0247	0.9668	0.8636	0.0332	0.9684	0.864	0.0316
Multiple Geometric Transformations									
Rotate + Resize	0.9236	0.7986	0.0764	0.9306	0.8125	0.0694	0.8148	0.7407	0.1852

Table 6.1 continued from previous page

Multiple Enhancement									
Sharpen + Median Filter	0.9753	0.8889	0.0247	0.9722	0.8472	0.0278	0.9672	0.864	0.0328

From Figures 6.9-6.16, it can be observed that for most of the attacks the values for NC, TAF are above 0.9 and 0.8 respectively, while values for BER are usually below 0.1. NC values for Median Filter are quite low but still above 0.8. These high values of NC and TAF; and low values of BER ensure high robustness of the scheme. Even in the simulation 3, when 30 images have been attacked with different attacks, the values of NC and TAF remain above 0.9 and 0.8, respectively. Simulation 1 of the proposed scheme has been compared to the recent single owner schemes in Table 6.2 in terms of robustness using parameter NC. The results have been compared for the images and attacks that were available in the results of existing schemes.

Table 6.2: Robustness comparison of Proposed Scheme with Existing Single Owner Schemes in terms of NC, for different images and against different attacks

Images	Roy and Pal (2017)	Murali and Sankaradass (2018)	Ernawan and Kabir (2020)	Hurrah et al. (2019)	Thanki et al. (2019)	Proposed Scheme
JPEG Compression						
Lena	-	0.85	-	-	-	0.9876
Lake	-	0.87	-	-	-	0.9829
Mandrill	-	0.82	-	-	-	0.9877
Peppers	0.8916	-	0.5876	-	0.9837	0.9889
Rotation						
Lena	-	0.79	-	-	-	0.9728
Peppers	0.5593	-	0.5864	-	-	0.9876
Lake	-	0.78	-	-	-	0.9629
Mandrill	-	0.79	-	-	-	0.9753
Median Filtering						
Lena	-	0.95	-	-	-	0.9523
Lake	-	0.87	-	-	-	0.8889
Mandrill	-	0.89	-	-	-	0.8941
Peppers	0.8055	-	-	-	-	0.8196

Cropping						
Lena	-	-	-	0.989	-	0.9844
Peppers	0.9657	-	-	-	-	0.9844
Gaussian Noise						
Lena	-	0.89	-	-	-	0.9629
Mandrill	-	0.83	-	-	-	0.9753
Lake	-	0.9	-	-	-	0.9722
Peppers	0.6412	-	-	-	-	0.9506
Sharpening						
Lena	-	0.87	-	0.975	-	0.9629
Peppers	0.9645	-	-	-	-	0.9723
Lake	-	0.92	-	-	-	0.9506
Mandrill	-	0.83	-	-	-	0.9352
Salt and Pepper Noise						
Lena	-	0.89	-	0.96	-	0.9753
Lake	-	0.91	-	-	-	0.9858
Mandrill	-	0.81	-	-	-	0.9877
Peppers	0.5852	-	-	-	-	0.9784
Speckle Noise						
Lena	-	-	-	0.97	-	0.9890
Poisson Noise						
Lena	-	-	-	0.96	-	0.9612

The results that were not available in the existing schemes have been marked with '-'.

It can be observed from Table 6.2 that for every attack, the results of proposed scheme are either better or atleast similar to the existing schemes. For rotation attack, there is a remarkable improvement as the maximum value for NC was till now provided by Murali and Sankaradass (2018), *i.e.* 0.7, that has been increased to above 0.9 in the proposed scheme.

Table 6.3 shows the comparison of robustness of the proposed scheme with existing schemes Liu and Wu (2011); Amiri and Moghaddam (2016) that work for multiple images with multiple owners. Parameters used for this comparison are NC and TAF.

It can be observed from Table 6.3 that the proposed scheme shows remarkably better robustness than the existing schemes for almost all the attacks, especially, cropping and rotation attacks. For

cropping, the NC results have increased to 0.99 from 0.6 (Liu and Wu (2011)) and 0.96 (Amiri and Moghaddam (2016)), while for TAF, the results have increased to 0.9 from 0.5(Liu and Wu (2011)) and 0.7 (Amiri and Moghaddam (2016)). Similarly, for rotation, the NC values have increased to 0.93 from 0.6 (Liu and Wu (2011)) and 0.8(Amiri and Moghaddam (2016)), while TAF have increased from 0.5(Liu and Wu (2011)) and 0.66 (Amiri and Moghaddam (2016)). For other image processing attacks, the performance is either better or atleast similar to the existing schemes.

Table 6.4 shows a qualitative comparison of the proposed scheme with two existing schemes Liu and Wu (2011) and Amiri and Moghaddam (2016). These schemes are chosen for the comparison as to the best of our knowledge, these are the only VC based copyright protection schemes that work for multiple images with multiple owners.

Table 6.3: Quantitative Comparison of the proposed scheme with existing multiple images schemes in terms of NC and TAF

	Average NC			Average TAF		
	Liu and Wu (2011)	Amiri and Moghaddam (2016)	Proposed	Liu and Wu (2011)	Amiri and Moghaddam (2016)	Proposed
JPEG (10%)	0.9929	0.9794	0.9876	0.8198	0.8087	0.9012
JPEG (30%)	0.9958	0.9928	0.9753	0.8223	0.8197	0.8889
JPEG (70%)	0.9969	0.9972	0.9629	0.8232	0.8223	0.8765
Crop (border 50 pixels)	0.6877	0.96	0.9956	0.5678	0.7927	0.9122
Crop (border 100 pixels)	0.6044	0.8786	0.9891	0.499	0.7225	0.9091
Noising (10 %)	0.8789	0.9606	0.9723	0.7257	0.7931	0.8472
Resizing (1/8)	0.9374	0.9804	0.9653	0.774	0.8095	0.8402
Rotation (5 degrees)	0.637	0.8009	0.9311	0.526	0.6613	0.8138
Sharpening	0.9967	0.9884	0.9514	0.8229	0.8161	0.8264

Table 6.4: Qualitative comparison of the proposed scheme with the existing schemes

	Meaningful Shares	Sharing Case	Multitple Images	Multiple Owners	Blindness	Extraction	Side Information	Robustness
Liu and Wu (2011)	No	(n+t+1,n+t+1)	Yes	Yes	Yes	Superimposition + Recovery	No	JPEG Compression, Blurring, Sharpening, Scaling, Cropping, Distortion, Noising
Amiri and Moghaddam (2016)	No	(n+2,n+2)	Yes	No	Yes	XOR Superimposition	Yes	JPEG Compression, Blurring, Sharpening, Resizing, Cropping, Distortion, Noising
Proposed Scheme	Yes	(k,n)	Yes	Yes	Yes	XOR Superimposition	No	JPEG Compression, Blurring, Sharpening, Resizing, Cropping, Distortion, Noising , Rotation, Median Filtering

Unlike the existing schemes, the proposed scheme creates meaningful shares, shows robustness against rotation attack and works for multiple images with multiple owners. Unlike Amiri and Moghaddam (2016), the proposed scheme does not use any side information. The watermark is retrieved just by XOR superimposition, while Liu and Wu (2011), an additional recovery technique was required to retrieve the watermark. The proposed scheme ensures security by generating meaningful shares which give no hint that some secret information is stored inside them. Also, there is no restriction on the watermark size. The proposed schemes ensures no false positive cases as LBP helps in storing image global information efficiently.

6.5 Conclusion of the Chapter

In this Chapter, we proposed an EVCS-based copyright protection scheme to protect the ownership of multiple images with multiple owners. Using SURF keypoints, LBP features and EVCS the scheme ensures strong robustness, perfect imperceptibility and security, respectively. The watermark can be retrieved blindly just by XOR-superimposition of the qualified ownership images. The watermark's size is not restricted to the size of the protected image and meaningful ownership images ensure security of the scheme. We performed simulations on different number of images and owners against different image processing attacks to test robustness of the scheme. For majority of the experiments, NC and TAF values of the extracted watermark are maintained above 0.9 and 0.8, respectively, and BER values are maintained below 0.1, which shows that the scheme has outstanding resistance to single as well as multiple attacks. A qualitative and quantitative comparison with the existing copyright protection schemes verifies the efficiency of the proposed scheme.

CHAPTER 7

Conclusion and Future Scope

This Chapter discusses the conclusion and future scope of this thesis.

7.1 Conclusions

The entire focus of this thesis is on the development of copyright protection and authentication schemes using VC approach. An improved authentication scheme based on WPD, VC and CA is proposed. The tampered areas are detected just by XOR-superimposition of shares, thus has less computational complexity . Experimental results and discussions demonstrate the efficiency of the proposed scheme in terms of imperceptibility, extraction of the hidden watermark with minimum complexity, high accuracy in tamper detection, better security due to meaningful shares, low storage cost and low transmission cost. Also, as compared to some reported authentication schemes based on VC, the scheme can directly generate meaningful authentication shares without any additional data hiding process. Tamper detection rate and tamper detection accuracy have been observed more than 99% for different images against different tamper attacks.

A secure and robust copyright protection scheme based on DCuT, K-means Clustering and *EVCS* is proposed. The selection of non fine scale layer DCuT coefficients enhance the robustness

of the scheme. Baker Map is used for scrambling host image and watermark to make the scheme secure. A codebook is proposed to create meaningful ownership shares, thereby ensuring security of the scheme. The computational cost is low as watermark can be retrieved blindly just by *XOR*-superimposition of the shares. Experiments have been performed on different images by doing different attacks to check robustness of the scheme. *NC* value of the extracted watermark is maintained at 0.99 or more, which shows that the scheme has outstanding resistance to attacks. The advantages of the proposed scheme are high robustness, imperceptibility, security and blind detection. The watermark's size is not restricted to the size of the protected image. Comparison with the state-of-art copyright protection schemes reveals that the proposed scheme gives better performance.

This scheme suffered from false positive cases. Thus an enhanced copyright protection scheme for color images is proposed that can handle false positive cases efficiently. An additional watermark is created from C_b, C_r channels of the image to handle the false positive cases. To prove the copyright, the watermarks can be retrieved by *OR*-superimposition of OS with MS and its rotated version. Experimental results have been performed on different images for different attacks. NC value of the extracted watermark is maintained at 0.99 or more while BER is maintained below 0.1, which shows that the scheme has outstanding resistance to attacks. The advantages of the proposed copyright protection scheme are that the watermark's size is not restricted to the size of the protected image; the self constructed watermark handles false positive cases, and meaningful shares ensure security of the scheme. Comparison with the other exiting copyright protection schemes for color images reveals that the proposed scheme gives better performance.

These schemes are extended to work for multiple images with multiple owners. An *EVCS*-based copyright protection scheme is proposed to protect the ownership of multiple images with multiple owners. Using *SURF* keypoints, *LBP* features and *EVCS* the scheme ensures strong robustness, perfect imperceptibility and security, respectively. The watermark can be retrieved blindly just by *XOR*-superimposition of the qualified ownership images. The watermark's size is not restricted to the size of the protected image and meaningful ownership images ensure security of the scheme. We performed simulations on different number of images and owners against different image processing attacks to test robustness of the scheme. For majority of the experiments, *NC* and *TAF* values of the extracted watermark are maintained above 0.9 and 0.8, respectively, and *BER* values are maintained below 0.1, which shows that the scheme has outstanding resistance to single as well as

multiple attacks. A qualitative and quantitative comparison with the existing copyright protection schemes verifies the efficiency of the proposed scheme.

7.2 Future Scope

This work has focused on copyright protection and authentication schemes based on *VC*. Four different schemes have been proposed by improving the gaps in existing schemes. However, there is still now a scope of improvement in these schemes. This section discusses a few possible improvements that can further enhance these schemes:

- In future, the creation of meaningful shares can be improved and automated by the use of Generative Adversarial Networks. This would save the effort and cost of using codebooks to create the shares. The networks can be trained to create new meaningful shares with a relationship that when superimposed, they should retrieve the watermark. Such networks would not require the use of cover images, as they possess the capabilities to generate new images that do not already exist but follow certain requirements.

- In our schemes, we create shares of size equal to the size of the host image. These schemes can be further extended to create shares of size lesser than the host image, by using Polynomial based *VC*. The pixels in the image blocks can be used to evaluate the coefficient values for the polynomial, whose result would represent the share pixel value. This would further help in saving the storage and transmission cost.

- The schemes can also be extended to videos, by analyzing the inter frame relationship and protecting them using the proposed schemes. Shares would be constructed for every frame and stored with the participants. The audio signals in the video can also be protected by *VC*. At the receiver's side, the superimposition results would prove the copyright and authenticity of the videos.

- Presently, the value of k, *i.e.* the minimum number of participants required for superimposition, is mutually decided by the owners and participants involved. A mathematical analysis and proof can be proposed to decide the value of k, that would help in ensuring security and provide a standard solution to every *VC* based scheme.

References

Abraham, J. and Paul, V. (2019). An imperceptible spatial domain color image watermarking scheme. *Journal of King Saud University-Computer and Information Sciences*, 31(1):125–133.

Agarwal, S. (2018). A review of image scrambling technique using chaotic maps. *International Journal of Engineering and Technology Innovation*, 8(2):77–98.

Al-Dahhan, R. R., Shi, Q., Lee, G. M., and Kifayat, K. (2019). Survey on revocation in ciphertext-policy attribute-based encryption. *Sensors*, 19(7):1695(1–22).

Al-Otum, H. M. (2014). Semi-fragile watermarking for grayscale image authentication and tamper detection based on an adjusted expanded-bit multiscale quantization-based technique. *Journal of Visual Communication and Image Representation*, 25(5):1064–1081.

Al-Otum, H. M. (2020). Secure and robust host-adapted color image watermarking using inter layered wavelet packets. *Journal of Visual Communication and Image Representation*, 66:102726(1–16).

Ali, M., Ahn, C. W., and Pant, M. (2018). An efficient lossless robust watermarking scheme by integrating redistributed invariant wavelet and fractional fourier transforms. *Multimedia Tools and Applications*, 77(10):11751–11773.

Amiri, T. and Moghaddam, M. E. (2016). A new visual cryptography based watermarking scheme using DWT and SIFT for multiple cover images. *Multimedia Tools and Applications*, 75(14):8527–8543.

Anwar, M. I. and Khosla, A. (2017). Vision enhancement through single image fog removal. *International Journal of Engineering Science and Technology*, 20(3):1075–1083.

Anwar, M. I., Khosla, A., and Singh, G. (2017). Visibility enhancement with single image fog removal scheme using a post-processing technique. In *Proceedings of International Conference on Signal Processing and Integrated Networks*, pages 280–285.

Aranda, M., Fdez-Valdivia, J., J.A., G., Garrido, A., Martínez Baena, J., and Rodríguez-Sánchez, R. (2000). Computer vision group at the university of granada. `http://decsai.ugr.es/cvg/dbimagenes/`.

Asuquo, P., Cruickshank, H., Morley, J., Ogah, C. P. A., Lei, A., Hathal, W., Bao, S., and Sun, Z. (2018). Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges, and countermeasures. *IEEE Internet of Things Journal*, 5(6):4778–4802.

Ateniese, G., Blundo, C., De Santis, A., and Stinson, D. R. (1996). Extended schemes for visual cryptography. *Theoretical Computer Science*, 250:1–16.

Bay, H., Ess, A., Tuytelaars, T., and Van Gool, L. (2008). Speeded-up robust features SURF. *Computer Vision and Image Understanding*, 110(3):346–359.

Benyoussef, M., Mabtoul, S., and Aboutajdine, D. (2014). Medical image watermarking for copyright protection based on visual cryptography. In *Proceedings of International Conference on Multimedia Computing and Systems*, pages 93–98.

Benyoussef, M., Mabtoul, S., El Marraki, M., and Aboutajdine, D. (2013). Blind invisible watermarking technique in DT-CWT domain using visual cryptography. In *Proceedings of International Conference on Image Analysis and Processing*, pages 813–822.

Benyoussef, M., Mabtoul, S., Marraki, M. E., and Aboutajdine, D. (2015). Robust ROI watermarking scheme based on visual cryptography: Application on mammograms. *Journal of Information Processing Systems*, 11(4):495–508.

Blundo, C., D'Arco, P., De Santis, A., and Stinson, D. R. (2003). Contrast optimal threshold visual cryptography schemes. *SIAM Journal on Discrete Mathematics*, 16(2):224–261.

Braik, M., Sheta, A. F., and Ayesh, A. (2007). Image enhancement using particle swarm optimization. In *Proceedings of World Congress on Engineering*, volume 1, pages 978–988.

Campbell, A. (2000). *The designer's lexicon: The illustrated dictionary of design, printing, and computer terms*. Chronicle Books.

Candès, E. J. and Donoho, D. L. (2004). New tight frames of curvelets and optimal representations of objects with piecewise C2 singularities. *Communications on Pure and Applied Mathematics*, 57(2):219–266.

Chang, C.-C., Chen, Y.-H., and Wang, H.-C. (2011). Meaningful secret sharing technique with authentication and remedy abilities. *Information Sciences*, 181(14):3073–3084.

Chang, C.-C., Hsiao, J.-Y., and Yeh, J.-C. (2002). A colour image copyright protection scheme based on visual cryptography and discrete cosine transform. *The Imaging Science Journal*, 50(3):133–140.

Chang, C.-C., Hsieh, Y.-P., and Lin, C.-H. (2008). Sharing secrets in stego images with authentication. *Pattern Recognition*, 41(10):3130–3137.

Chang, C.-C., Lin, P.-Y., Wang, Z.-H., and Li, M. (2010). A sudoku-based secret image sharing scheme with reversibility. *Journal of Communications*, 5(1):5–12.

Chen, T.-H., Chang, C.-C., Wu, C.-S., and Lou, D.-C. (2009). On the security of a copyright protection scheme based on visual cryptography. *Computer Standards & Interfaces*, 31(1):1–5.

Chuang, J.-C. and Hu, Y.-C. (2011). An adaptive image authentication scheme for vector quantization compressed image. *Journal of Visual Communication and Image Representation*, 22(5):440–449.

Cruickshank, H. (1996). *A security system for satellite networks*. IET.

Devi, B. P., Singh, K. M., and Roy, S. (2016). A copyright protection scheme for digital images based on shuffled singular value decomposition and visual cryptography. *SpringerPlus*, 5(1):1091(1–22).

Driebe, D. J. (1999). *Fully chaotic maps and broken time symmetry*, volume 4. Springer Science & Business Media.

Ernawan, F. and Kabir, M. N. (2020). A block-based RDWT-SVD image watermarking method using human visual system characteristics. *The Visual Computer*, 36(1):19–37.

Eslami, Z. and Ahmadabadi, J. Z. (2011). Secret image sharing with authentication-chaining and dynamic embedding. *Journal of Systems and Software*, 84(5):803–809.

Fares, K., Amine, K., and Salah, E. (2020). A robust blind color image watermarking based on fourier transform domain. *Optik*, 208:164562(1–9).

Fatahbeygi, A. and Tab, F. A. (2019). A highly robust and secure image watermarking based on classification and visual cryptography. *Journal of Information Security and Applications*, 45:71–78.

Fox, R. F. (1997). Construction of the jordan basis for the baker map. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 7(2):254–269.

Gangopadhyay, S., Gangopadhyay, A. K., Pollatos, S., and Stănică, P. (2017). Cryptographic boolean functions with biased inputs. *Cryptography and Communications*, 9(2):301–314.

Ghanekar, U., Singh, A. K., and Pandey, R. (2009). A contrast enhancement-based filter for removal of random valued impulse noise. *IEEE Signal Processing Letters*, 17(1):47–50.

Hénon, M. (1976). A two-dimensional mapping with a strange attractor. In *The Theory of Chaotic Attractors*, pages 94–102. Springer.

Hou, Y.-C. (2002). Copyright protection based on visual cryptography. *Proceedings of SCI*, 9:104–109.

Hou, Y.-C. and Chen, P.-M. (2000). An asymmetric watermarking scheme based on visual cryptography. In *Proceedings of IEEE International Conference on Signal Processing*, volume 2, pages 992–995.

Hou, Y.-C. and Huang, P.-H. (2012). An ownership protection scheme based on visual cryptography and the law of large numbers. *International Journal of Innovative Computing*, (6):4147–4156.

Hou, Y. C., Tseng, A.-Y., Quan, Z.-Y., and Liu, H.-J. (2016). An IPR protection scheme based on wavelet transformation and visual cryptography. *Turkish Journal of Electrical Engineering & Computer Sciences*, 24(5):4063–4082.

Hsieh, S.-L., Hsu, L.-Y., and Tsai, I.-J. (2005). A copyright protection scheme for color images using secret sharing and wavelet transform. In *Proceedings of World Academy of Science, Engineering and Technology*, volume 10, pages 3172 – 3178.

Hsu, C.-S. and Hou, Y.-C. (2005). Copyright protection scheme for digital images using visual cryptography and sampling methods. *Optical Engineering*, 44(7):077003(1–10).

Hurrah, N. N., Parah, S. A., Loan, N. A., Sheikh, J. A., Elhoseny, M., and Muhammad, K. (2019). Dual watermarking framework for privacy protection and content authentication of multimedia. *Future Generation Computer Systems*, 94:654–673.

Hwang, R.-J. (2000). A digital image copyright protection scheme based on visual cryptography. *Tamkang Journal of Science and Engineering*, 3(2):97–106.

Ilachinski, A. (2001). *Cellular automata: a discrete universe*. World Scientific Publishing Company.

Ito, R., Kuwakado, H., and Tanaka, H. (1999). Image size invariant visual cryptography. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 82(10):2172–2177.

Jensen, A. and la Cour-Harbo, A. (2001). *Ripples in mathematics: the discrete wavelet transform*. Springer Science & Business Media.

Jiang, P., Zhao, S., and Cheng, S. (2015). Rotational invariant LBP-SURF for fast and robust image matching. In *Proceedings of IEEE International Conference on Signal Processing and Communication Systems*, pages 1–7.

Karami, E., Prasad, S., and Shehata, M. (2017). Image matching using SIFT, SURF, BRIEF and ORB: performance comparison for distorted images. *arXiv preprint arXiv:1710.02726*.

Kutter, M. and Petitcolas, F. A. (1999). Fair benchmark for image watermarking systems. In *Proceedings of SPIE Security and Watermarking of Multimedia Contents*, volume 3657, pages 226–239.

Larson, E. C. and Chandler, D. (2010). Categorical image quality CSIQ database. `http://vision.eng.shizuoka.ac.jp/mod/page/view.php?id=23`.

Lee, T.-Y. and Lin, S. D. (2008). Dual watermark for image tamper detection and recovery. *Pattern Recognition*, 41(11):3497–3506.

Li, C., Zhang, A., Liu, Z., Liao, L., and Huang, D. (2015). Semi-fragile self-recoverable watermarking algorithm based on wavelet group quantization and double authentication. *Multimedia Tools and Applications*, 74(23):10581–10604.

Li, M., Xiao, D., and Zhang, Y. (2016). Attack and improvement of the fidelity preserved fragile watermarking of digital images. *Arabian Journal for Science and Engineering*, 41(3):941–950.

Li, P., Ma, P.-J., Su, X.-H., and Yang, C.-N. (2012). Improvements of a two-in-one image secret sharing scheme based on gray mixing model. *Journal of Visual Communication and Image Representation*, 23(3):441–453.

Lin, C.-C. and Tsai, W.-H. (2004). Secret image sharing with steganography and authentication. *Journal of Systems and Software*, 73(3):405–414.

Lin, S. D., Kuo, Y.-C., and Huang, Y.-H. (2006). An image watermarking scheme with tamper detection and recovery. In *Proceedings of IEEE International Conference on Innovative Computing, Information and Control*, volume 3, pages 74–77.

Lin, S. D., Lin, J.-H., and Chen, C.-Y. (2011). A ROI-based semi-fragile watermarking for image tamper detection and recovery. *International Journal of Innovative Computing, Information and Control*, 7(12):6875–6888.

Lin, S. D. and Yang, Z.-L. (2011). Hierarchical fragile watermarking scheme for image authentication. *Intelligent Automation & Soft Computing*, 17(2):245–255.

Liu, F. and Wu, C.-K. (2011). Robust visual cryptography-based watermarking scheme for multiple cover images and multiple owners. *IET Information Security*, 5(2):121–128.

Liu, F. and Yan, W. Q. (2014). Visual cryptography for image processing and security. *Springer International Publishing*.

Liu, Y., Tang, S., Liu, R., Zhang, L., and Ma, Z. (2018). Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Systems with Applications*, 97:95–105.

Lou, D.-C., Chen, H.-H., Wu, H.-C., and Tsai, C.-S. (2011). A novel authenticatable color visual secret sharing scheme using non-expanded meaningful shares. *Displays*, 32(3):118–134.

Lou, D.-C., Tso, H.-K., and Liu, J.-L. (2007). A copyright protection scheme for digital images using visual cryptography technique. *Computer Standards & Interfaces*, 29(1):125–131.

MacQueen, J. (1967). Some methods for classification and analysis of multivariate observations. In *Proceedings of Berkeley symposium on mathematical statistics and probability*, volume 1, pages 281–297.

Makbol, N. M., Khoo, B. E., and Rassem, T. H. (2016). Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image processing*, 10(1):34–52.

Muhammad, M. A., Zadeh, P., and Ayesh, A. (2017). Improving security in bring your own device (byod) environment by controlling access. In *Proceedings of Faculty of Technology Wide Conference*. ACM.

Murali, P. and Sankaradass, V. (2018). An efficient ROI based copyright protection scheme for digital images with svd and orthogonal polynomials transformation. *Optik*, 170:242–264.

Naor, M. and Pinkas, B. (1997). Visual authentication and identification. In *Proceedings of Springer Annual International Cryptology Conference*, pages 322–336.

Naor, M. and Shamir, A. (1994). Visual cryptography. In *Proceedings of Springer Workshop on the Theory and Application of of Cryptographic Techniques*, pages 1–12.

Ojala, T., Pietikäinen, M., and Harwood, D. (1996). A comparative study of texture measures with classification based on featured distributions. *Pattern Recognition*, 29(1):51–59.

Otsu, N. (1979). A threshold selection method from gray-level histograms. *IEEE Transactions on Systems, Man, and Cybernetics*, 9(1):62–66.

Pandey, R. and Ghanekar, U. (2015). Denoising of colour images using window contrast enhancement and vector alignment. *AEU-International Journal of Electronics and Communications*, 69(2):523–528.

Peng, Y., Niu, X., Fu, L., and Yin, Z. (2018). Image authentication scheme based on reversible fragile watermarking with two images. *Journal of Information Security and Applications*, 40:236–246.

Percival, D. B. and Walden, A. T. (2000). *Wavelet methods for time series analysis*, volume 4. Cambridge university press.

Prabhakar, C. and Kumar, P. P. (2012). LBP-SURF descriptor with color invariant and texture based features for underwater images. In *Proceedings of Indian Conference on Computer Vision, Graphics and Image Processing*, pages 1–8.

Preda, R. O. (2013). Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain. *Measurement*, 46(1):367–373.

Rawat, S. and Raman, B. (2012). A publicly verifiable lossless watermarking scheme for copyright protection and ownership assertion. *AEU-International Journal of Electronics and Communications*, 66(11):955–962.

Roy, S. and Pal, A. K. (2017). A robust blind hybrid image watermarking scheme in RDWT-DCT domain using arnold scrambling. *Multimedia Tools and Applications*, 76(3):3577–3616.

Salameh, H. B., Almajali, S., Ayyash, M., and Elgala, H. (2017). Security-aware channel assignment in iot-based cognitive radio networks for time-critical applications. In *Proceedings of IEEE International Conference on Software Defined Systems*, pages 43–47.

Salameh, H. B., Almajali, S., Ayyash, M., and Elgala, H. (2018). Securing delay-sensitive cognitive radio iot communications under reactive jamming attacks: Spectrum assignment perspective. In *Proceedings of IEEE International Conference on Software Defined Systems*, pages 20–24.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11):612–613.

Shao, Z., Shang, Y., Zeng, R., Shu, H., Coatrieux, G., and Wu, J. (2016). Robust watermarking scheme for color image based on quaternion-type moment invariants and visual cryptography. *Signal Processing: Image Communication*, 48:12–21.

Shen, H. and Chen, B. (2012). From single watermark to dual watermark: a new approach for image watermarking. *Computers & Electrical Engineering*, 38(5):1310–1324.

Shie, S.-C. and Lin, S. (2008). Improving robustness of visible image watermarks. *The Imaging Science Journal*, 56(1):23–28.

Shojanazeri, H., Adnan, W. A. W., Ahmad, S. M. S., and Rahimipour, S. (2017). Authentication of images using zernike moment watermarking. *Multimedia Tools and Applications*, 76(1):577–606.

Singh, A. K., Kumar, B., Singh, S. K., Ghrera, S., and Mohan, A. (2018). Multiple watermarking technique for securing online social network contents using back propagation neural network. *Future Generation Computer Systems*, 86:926–939.

Singh, D. and Singh, S. K. (2017a). Dct based efficient fragile watermarking scheme for image authentication and restoration. *Multimedia Tools and Applications*, 76(1):953–977.

Singh, D. and Singh, S. K. (2017b). DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. *Multimedia Tools and Applications*, 76(11):13001–13024.

Sridhar, S. and Baskaran, R. (2015). Efficient routing in mobile adhoc networks emphasizing quality of service by trust & energy based aodv. *Journal of Communications Software and Systems*, 11(1):1–7.

Srividhya, S., Sathishkumar, R., and Sudha, G. F. (2016). Implementation of tioisss with meaningful shadows and with an additional authentication image. *Journal of Visual Communication and Image Representation*, 38:284–296.

Thanki, R., Kothari, A., and Trivedi, D. (2019). Hybrid and blind watermarking scheme in DCuT–RDWT domain. *Journal of Information Security and Applications*, 46:231–249.

Tiwari, A., Sharma, M., and Tamrakar, R. K. (2017). Watermarking based image authentication and tamper detection algorithm using vector quantization approach. *AEU-International Journal of Electronics and Communications*, 78:114–123.

Truong, N. B., Sun, K., Lee, G. M., and Guo, Y. (2019). Gdpr-compliant personal data management: A blockchain-based solution. *IEEE Transactions on Information Forensics and Security*, 15:1746–1761.

Ulutas, G., Ulutas, M., and Nabiyev, V. V. (2013). Secret image sharing scheme with adaptive authentication strength. *Pattern Recognition Letters*, 34(3):283–291.

Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J. J., and Su, J. K. (2001). Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. *IEEE Communications Magazine*, 39(8):118–126.

Wang, C.-C., Tai, S.-C., and Yu, C.-S. (2000). Repeating image watermarking technique by the visual cryptography. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 83(8):1589–1598.

Wang, M.-S. and Chen, W.-C. (2007). Digital image copyright protection scheme based on visual cryptography and singular value decomposition. *Optical Engineering*, 46(6):067006(1–4).

Wang, M.-S. and Chen, W.-C. (2009). A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography. *Computer Standards & Interfaces*, 31(4):757–762.

Weber, A. G. (1997). The USC-SIPI image database version 5. *USC-SIPI Report*, 315(1).

Weir, J. and Yan, W. (2010). A comprehensive study of visual cryptography. In *Transactions on Data Hiding and Multimedia Security V*, pages 70–105. Springer.

Weir, J. P. (2011). *Visual cryptography and its applications*. Bookboon.

Wolfram, S. (1983). Statistical mechanics of cellular automata. *Reviews of Modern Physics*, 55(3):601.

Wu, C.-C., Kao, S.-J., Kuo, W.-C., and Hwang, M.-S. (2008). Enhance the image sharing with steganography and authentication. In *Proceedings of IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pages 1177–1181.

Wu, X. and Sun, W. (2013a). Robust copyright protection scheme for digital images using overlapping DCT and SVD. *Applied Soft Computing*, 13(2):1170–1182.

Wu, X. and Sun, W. (2013b). Secret image sharing scheme with authentication and remedy abilities based on cellular automata and discrete wavelet transform. *Journal of systems and software*, 86(4):1068–1088.

Wu, X. and Yang, C.-N. (2019). Partial reversible AMBTC-based secret image sharing with steganography. *Digital Signal Processing*, 93:22–33.

Xia, Z., Wang, X., Zhou, W., Li, R., Wang, C., and Zhang, C. (2019). Color medical image lossless watermarking using chaotic system and accurate quaternion polar harmonic transforms. *Signal Processing*, 157:108–118.

Xiong, L., Zhong, X., and Yang, C.-N. (2020). DWT-SISA: A secure and effective discrete wavelet transform-based secret image sharing with authentication. *Signal Processing*, pages 107571(1–9).

Xue, M., Yuan, C., Liu, Z., and Wang, J. (2019). SSL: A novel image hashing technique using SIFT keypoints with saliency detection and LBP feature extraction against combinatorial manipulations. *Security and Communication Networks*, 2019:9795621(1–18).

Yampolskiy, R. V., Rebolledo-Mendez, J. D., and Hindi, M. M. (2014). Password protected visual cryptography via cellular automaton rule 30. In *Springer Transactions on Data Hiding and Multimedia Security IX*, pages 57–67.

Yang, C.-N. and Chen, T.-S. (2005a). Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion. *Pattern Recognition Letters*, 26(2):193–206.

Yang, C.-N. and Chen, T.-S. (2005b). Extended visual secret sharing schemes with high-quality shadow images using gray sub pixels. In *Proceedings of International Springer Conference Image Analysis and Recognition*, pages 1184–1191.

Yang, C.-N. and Chen, T.-S. (2006). Reduce shadow size in aspect ratio invariant visual secret sharing schemes using a square block-wise operation. *Pattern Recognition*, 39(7):1300–1314.

Yang, C.-N., Chen, T.-S., Yu, K. H., and Wang, C.-C. (2007). Improvements of image sharing with steganography and authentication. *Journal of Systems and Software*, 80(7):1070–1076.

Yang, C.-N., Ouyang, J.-F., and Harn, L. (2012). Steganography and authentication in image sharing without parity bits. *Optics Communications*, 285(7):1725–1735.

Yang, H.-y., Qi, S.-r., Niu, P.-p., and Wang, X.-y. (2020). Color image zero-watermarking based on fast quaternion generic polar complex exponential transform. *Signal Processing: Image Communication*, 82:115747(1–19).

Zarepour-Ahmadabadi, J., Ahmadabadi, M. S., and Latif, A. (2016). An adaptive secret image sharing with a new bitwise steganographic property. *Information Sciences*, 369:467–480.

Zhu, C., Bichot, C.-E., and Chen, L. (2013). Image region description using orthogonal combination of local binary patterns enhanced with color information. *Pattern Recognition*, 46(7):1949–1963.