

DESIGN AND IMPLEMENTATION OF THE ROBUST WATERMARKING TECHNIQUE FOR THE RAW DIGITAL VIDEO BASED ON CDMA

Submitted By:

MONICA GUPTA

University Roll No. : 8730

Class Roll No. : 11/E&C/04

M. E. (ECE)

FULL-TIME

MAJOR PROJECT REPORT

Submitted in partial fulfillment of requirements for the award of the degree of

**Master of Engineering
In
Electronics and Communication Engineering**

Under the supervision and guidance of:

Mr. JEEBANANDA PANDA

Department of Electronics and Communication



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGG.
DELHI COLLEGE OF ENGINEERING, DELHI-110042

(Session 2004-2006)

CERTIFICATE

This is to certify that **Ms. Monica Gupta** , University Roll No. : **8730** and Class Roll No. **11/E&C/04** , have successfully carried out the project work titled ***“DESIGN & IMPLEMENTATION OF A ROBUST WATERMARKING TECHNIQUE FOR THE RAW DIGITAL VIDEO BASED ON CDMA”*** as a partial requirement for the award of Degree of Master Of Engineering, in Electronics & Communications Department , by Delhi University, New Delhi and is a record of bonafide work carried out and completed under my supervision and guidance during the academic session 2004-2006. The matter contained in this thesis has not been submitted elsewhere for award of any other degree.

Dr. A. Bhattacharyya
Prof. & Head
Deptt. of E&C Engg.
Delhi College of Engg.
Delhi-110042

Mr. Jeebananda Panda
Lecturer(Project Guide)
Deptt. of E&C Engg.
Delhi College of Engg.
Delhi-110042

ACKNOWLEDGEMENT

I am very grateful and thankful to all those people who extended their support to complete my project.

I express my gratitude to our esteemed guide Mr. Jeebananda Panda , Lecturer in Deptt. of Electronics and Communication Engg, D.C.E. Delhi, who assisted me throughout my project.

I would be failing in my duties, if I did not thank Prof. Asok Bhattacharyya, Head of the Deptt. of Electronics and Communication Engineering, D.C.E. Delhi, for inspiring me to strive to achieve the best.

I extend my special thanks to Mr. Akash Tayal, Lecturer IGIT, Delhi for his valuable help and guidance. If the present work is sound and scientifically correct, it is mostly his merit. He guided me every step of the way, always providing me with a higher-level view and a clear direction to follow.

I also take this opportunity to thank the management and the Lab assistants of DCE for permitting me and providing me the necessary facilities to carry out my project.

Monica Gupta

University Roll No. : 8730

Class Roll. No.: 11/E&C/04

ABSTRACT

The focus of the project entitled "DESIGN AND IMPLEMENTATION OF THE ROBUST WATERMARKING TECHNIQUE FOR THE RAW DIGITAL VIDEO BASED ON CDMA " is to ultimately embed a robust Watermark in the digital Video that will identify its Owner unambiguously.

Spread spectrum has been used as a technique for secure communications for a long time. For still image Watermarking , spread spectrum has been the method of choice for some time. In this project we argue that spread spectrum in the form of CDMA has a more natural application in the Watermarking of uncompressed digital Video. The reason for this sentiment is that digital Video, by virtue of its time-space property, fits the direct sequence spread spectrum more readily. The problem, however, is that conventional CDMA achieves its data-hiding capability by a massive increase in bit-rate. Successful implementation of CDMA for Video Watermarking, therefore, requires a reformulation of the concept.

The digital Video, here, is modeled as a bitplane stream along the time axis. Previous research indicates that lower bitplanes of the digital frames have to be modified in order to embed the information in a reliable and robust way.

In spread spectrum communications, a narrow-band signal is spread across a wide band of frequencies. This can be accomplished by modulating the narrow-band signal (the Watermark information in our case) with a wide-band signal, such as Gaussian noise. The spread Watermark signal is similar to the noise already present in the image signal and therefore hard to detect. This led to the development of the discussed Watermarking scheme.

Using a modified m -sequence, bitplanes of specific order are pseudorandomly marked for Watermarking. The desired Watermark is mapped to a single bitplane and spread via another 2D m -sequence, not necessarily related to the first one, along a stream parallel to that of the Video. The tagged planes are removed and replaced by the spread Watermark.

Several types of attacks (regular and/or random frame removal.) have been preformed on the Watermarked Video to check the reliability & robustness of the developed technique. The results show that the above approach resists noise as well as attacks on destroying synchronization at the Watermark detector.

TABLE OF CONTENTS

Topics	Page Nos.
1. INTRODUCTION TO THE WORLD OF WATERMARKING.....	1
1.1 HISTORY	
1.2 DIGITAL WATERMARK	
1.3 DIGITAL DISTRIBUTION & NEED FOR DIGITAL WATERMARKING	
1.4 COPYRIGHT PROTECTION	
1.5 IMAGE AUTHENTICATION & DATA INTEGRITY	
1.6 DATA HIDING AND IMAGE LABELING	
1.7 DIFFERENCES AMONG WATERMARKING ,STEGANOGRAPHY & CRYPTOGRAPHY	
1.8 ASPECTS & REQUIREMENTS OF WATERMARKING PROBLEM	
2. DIGITAL VIDEO & VIDEO WATERMARKING	7
2.1 VIDEO WATERMARKING	
2.2 TECHNIQUE	
2.2.1 REQUIREMENTS	
2.2.2 HOW IT WORKS	
2.3 SOME IMPORTANT ISSUES	
2.4 EXPLORING CDMA FOR WATERMARKING OF DIGITAL VIDEO	
2.4.1 INTRODUCTION	
2.4.2 CDMA AND ITS RELEVANCE TO WATERMARKING	
2.4.3 DEVELOPMENT OF CDMA WATERMARKING MODEL	
2.4.4 ROBUSTNESS ISSUE : NOISE AND SYNCHRONIZATION	
2.5 WATERMARKING APPLICATIONS	
3. WATERMARKING EVERYTHING.....	20
3.1 APPLICATIONS	
3.2 TYPES OF WATERMARK	
3.3 CLASSES OF WATERMARKING	
3.4 FEATURES OF WATERMARKS	
3.5 KEY POINTS TO REMEMBER	

4. LITERATURE REVIEW.....27

4.1 BASIC PRINCIPLE OF DIRECT SEQUENCE SPREAD SPECTRUM

4.1.1 SPREADING

4.1.2 DESPREADING

4.2 PSEUDO-RANDOM NOISE

4.2.1 PSEUDO RANDOM

4.2.2 CODE LENGTH

4.3 PROPERTIES OF SPREAD SPECTRUM EXPLOITED FOR WATERMARKING

5. THE WATERMARKING OF DIGITAL VIDEO.....34

RESEARCH WORK :

5.1 OBJECTIVE OF THE PROJECT

5.2 OVERVIEW OF THE PROJECT

5.3 STAGE I : WATERMARK INSERTION

5.3.1 MODEL OF THE STAGE

5.3.2 MATLAB SIMULATION

5.3.3 RESULTS

5.4 STAGE II : ATTACKS ON WATERMARKED DIGITAL VIDEO

5.4.1 MODEL OF THE STAGE

5.4.2 MATLAB SIMULATION

5.4.3 RESULTS

5.5 STAGE III : WATERMARK DETECTION

5.5.1 MODEL OF THE STAGE

5.5.2 MATLAB SIMULATION

5.5.3 RESULTS

6 CONCLUSION.....242

6.1 PERFORMANCE EVALUATION (FROM PROJECT SIMULATION)

6.1.1 SUMMARY

6.1.2 EXPERIMENTAL RESULTS

6.2 PROJECT IMPLICATIONS

6.3 FUTURE SCOPE

LIST OF TABLES

LIST OF FIGURES

APPENDIX

GLOSSARY

REFERENCES

1. INTRODUCTION TO THE WORLD OF WATERMARKING

*A **Watermark** is the one which is added imperceptibly to the cover signal in order to convey the hidden data. It is a label applied to an image for various purposes, one being proof of ownership.*

*The process of embedding information into another object or signal is termed as **Watermarking**.*

HISTORY

First watermark related publications date back to 1979. However, it was only in 1990 that it gained a large international interest.

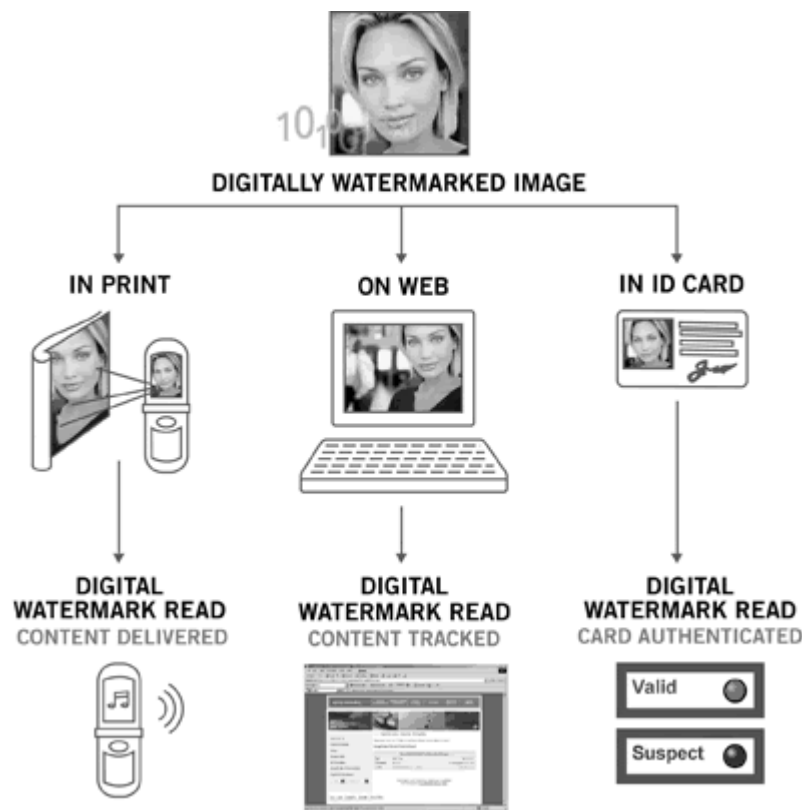
With the growth of the internet & the immediate availability of computing resources to everyone, “Digitized property “can be reproduced & instantaneously distributed without quality loss at basically any cost. Until now, intellectual property (IP) and value has always been bound to some physical container that could not be easily duplicated, thereby guaranteeing that the creator benefits from his work.

As audio, video & other works become available in digital form, it may be that the ease with which perfect copies can be made will lead to large-scale unauthorized copying which will undermine the music, film, book and software publishing industries.

One technical way to make law enforcement & copyright protection for digital media possible and practical is digital watermarking which is aimed to automatically detect & possibly also prosecute copyright infringement. There has therefore been significant recent research into “watermarking”(hiding copyright messages) and “fingerprinting “ (hiding serial numbers or a set of characteristics that tend to distinguish an object from other similar objects): the idea is that the latter can be used to detect copyright violators and the former to prosecute them.

DIGITAL WATERMARK

A **Digital Watermark** is a special message embedded in an image, whether it is a photo, video or other digital content. Watermarking technologies embeds these "imperceptible" messages by making subtle changes to the data of the original digital content. These watermarks can then be "read" to validate original content and/or deliver an action, such as delivering content to a mobile phone.



The change to the media is so subtle that such digital watermarks are considered imperceptible.

Digital watermarking describes methods and technologies that allow hiding information, for example a number or text, in digital media, such as images, video and audio. The embedding takes place by manipulating the content of the digital data that means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are *imperceptible*. For images this means that the modifications of the pixel values have to be invisible. Furthermore, the watermark has to be *robust* or *fragile*,

depending on the application. With robustness we refer to the capability of the watermark to resist to manipulations of the media, such as lossy compression, scaling, and cropping, just to enumerate some. Fragility means that the watermark should not resist tampering, or only up to a certain extent

DIGITAL DISTRIBUTION & NEED FOR DIGITAL WATERMARKING

The digital representation of audio signals, images, and video has become popular due to the ease of transmitting digital data and copying without loss of quality. However, unauthorized copying and distribution of digital data is simplified, too. For this reason, researchers have begun to investigate several methods of copy protection. It was realized that common cryptographic means are not sufficient since once the data is decrypted and displayed (in the case of images, and video, for example) the data can then be saved, modified etc. One potential area to solve this issue is Digital Watermarking.

Using this technique the imperceptible embedding of information into multimedia data, in the case of this project, digital images, takes place. The information remains detectable, as long as the quality of the content itself is not rendered severely perceptually degraded. Perceptible in the case of the images in this project refers to the Human Visual System (HVS). The computer will of course view the two images differently, but the user of the scheme should see as little as possible change in their image.

COPYRIGHT PROTECTION

The goal of watermarking for copyright protection is to embed a “mark “ into the image data that can identify the copyright holder of the work. Together with owner identification, one might also want to embed a mark (or fingerprint) identifying the buyer of a work for circulation tracking. The mark can be a registered number (like the UPC found on compact disc media) , a text message or graphical logo, or some unique pattern (similar to a DNA fingerprint).The term watermark stems from the ancient art of marking paper with a logo for the same purpose.

Digital watermarks can either be perceptible or imperceptible. Visible image watermarks, often the logo of the copyright holder, can be easily apply to the image but are hard to remove. Mintzer describes a successful implementation of visible image

watermarking. Many applications require the watermark to be invisible, however this work focuses on invisible watermarks in digital images only.

The embedded , invisible watermark has to be robust against common image processing operations like image compression(e.g. JPEG) , image filtering (Edge enhancement, contract enhancement,...) and geometrical transformations (e.g. cropping ,scaling ,...). Therefore, the watermark can not be stored in the file format, but has to be embedded into the image data itself. In order to establish a proof of ownership in a trial, a watermarking scheme also has to be secure against intentional malicious attacks , here, cryptographic techniques and statistical properties of pseudo –random numbers play an essential role.

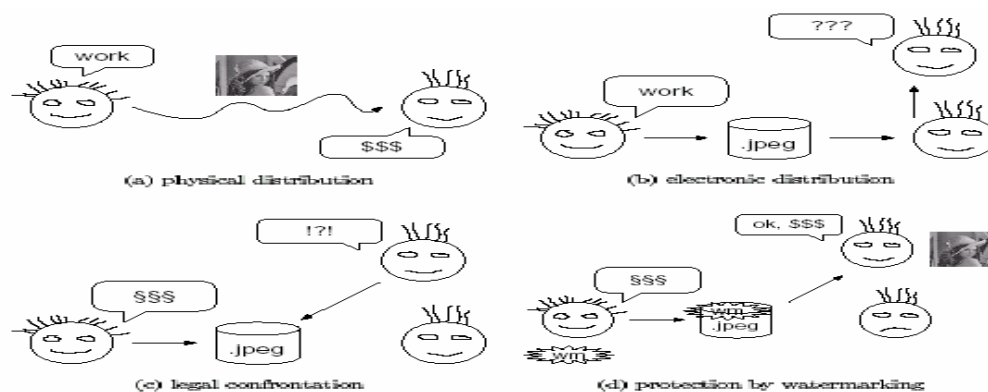


Figure 1.1: Intellectual property transfer between the creator and the customers of a work. (a) The photography is distributed traditionally and therefore hard to duplicate or manipulate. The clients pay for the work of the IP creator. (b) The work is distributed in electronic, digitized form. Making copies is cheap and easy, there seems to be no reason for a third party to pay royalties to the creator of the work. (c) The creator has difficulties to track copies of his digitized work and claim ownership in a legal trial. (d) A watermark can be used to convince the IP customers to pay the royalties without limiting usage of the work. In addition, a watermark may provide extra information and guarantee data integrity.

IMAGE AUTHENTICATION & DATA INTEGRITY

Another need for watermarking is for “image authentication” & “temper detection”.

Digital photographs are being used more and more often as court evidence nowadays. Here, watermarking is used to detect significant modification of the image. Digital image are susceptible to seamless modifications from sophisticated image processing applications. Watermarks can be used here as a means to verify the genuineness of an image. Verification watermarks are required to be fragile, so that any modification to the image will destroy (or detectable alter) the mark. Unlike cryptographic message digests which can only validate identical copies, watermarking for image authentication should tolerate some well-defined image distortion (e.g. file format conversion, re-sampling, re-compression or progressive transmission).

DATA HIDING AND IMAGE LABELING

Data hiding or steganography tries to invisibly embed the maximum amount of data into a host signal (e.g. an image). This allows communication using often enciphered messages without attracting the attention of the third party. typically, robustness requirements are low for steganographic purposes, instead invisibility and capacity are of prime importance.

Image labeling is an application where information about the image content is encoded as a watermark and inserted into the image to assist image retrieval from a database or provide extra information to the viewer.

DIFFERENCES AMONG WATERMARKING , STEGANOGRAPHY & CRYPTOGRAPHY

While *cryptography* is about protecting the content of messages (their meaning), steganography is about concealing their very existence. It comes from Greek roots, literally means 'covered writing', and is usually interpreted to mean hiding information in other information. Examples include sending a message to a spy by marking certain letters in a newspaper using invisible ink, and adding sub-perceptible echo at certain places in an audio recording. It is often thought that communications may be secured by encrypting the traffic, but this has rarely been adequate in practice. Æneas the Tactician, and other classical writers, concentrated on methods for hiding messages rather than for enciphering them; and although modern cryptographic techniques started to develop during the Renaissance, we find in 1641 that John Wilkins still preferred hiding over ciphering because it arouses less suspicion. This preference persists in many operational contexts to this day. For example, an encrypted email message between a known drug dealer and somebody not yet under suspicion, or between an employee of a defense contractor and the embassy of a hostile power, has obvious implications.

As the purpose of *steganography* is having a covert communication between two parties whose existence is unknown to a possible attacker, a successful attack consists in detecting the existence of this communication (e.g., using statistical analysis of images with and without hidden information). *Watermarking*, as opposed to steganography, has the (additional) requirement of robustness against possible attacks. In this context, the term 'robustness' is still not very clear; it mainly depends on the application. Copyright marks do

not always need to be hidden, as some systems use *visible digital watermarks*, but most of the literature has focused on imperceptible (e.g., invisible, inaudible) digital watermarks which have wider applications. Visible digital watermarks are strongly linked to the original paper watermarks which appeared at the end of the XIII century to differentiate paper makers of that time. Modern visible watermarks may be visual patterns (e.g., a company logo or copyright sign) overlaid on digital images. The intent of use is also different: the payload of a watermark can be perceived as an attribute of the cover-signal (e.g., copyright information, license, ownership, etc.). In most cases the information hidden using steganographic techniques is not related at all to the cover. These differences in goal lead to very different hiding techniques.

ASPECTS & REQUIREMENTS OF WATERMARKING PROBLEM:

- ✚ It should be **difficult to insert a false watermark** and the watermarking scheme should be able to indicate regions where alterations in the image have taken place.
- ✚ It should be possible to generate **large number of the watermarks** and the insertion of multiple watermarks should be handled properly.
- ✚ For data hiding and image labeling purposes, the **maximum capacity** of embedded message is of prime importance. Image labeling techniques require highly localized embedding of watermark information which rules out methods that operate on the entire image.
- ✚ As for cryptography, watermarking methods have to obey the **Kerckhoff principle** which means that security and robustness claims have to take into consideration that the algos for watermarking embedding and extraction are known in detail.
- ✚ The **message capacity**, that is the number of bits that can be reliably embedded in the image data, is fairly limited. For copyright protection applications that involve identification of the copyright holder as well as the identification of the licensee of the image, different lower capacity bounds have been proposed by **Piva & Kutter**.

2. DIGITAL VIDEO & VIDEO WATERMARKING

Video watermarking technology enables to hide invisible data in digital or analog video. This data can be used for tracking, fingerprinting, copyright infringement detection or any other application that requires some hidden data.

VIDEO WATERMARKING

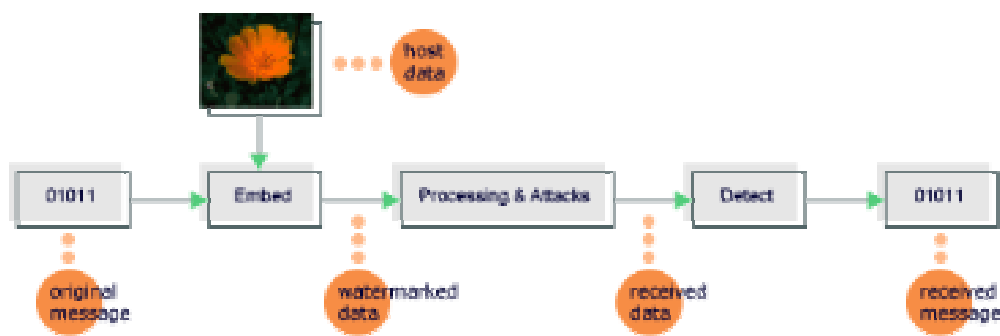


Figure 2.1

TECHNIQUE

Video watermarking can be achieved by either applying still image technologies to each frame of the movie or using dedicated methods which exploit inherent features of the video sequence.

REQUIREMENT

One of the primary requirements of video watermarking schemes is their robustness to unintentional attacks while avoiding the introduction of disturbing artifacts. The most important unintentional attack on video is lossy compression. In the production chain, compression is usually applied before video broadcasting or before transferring the video to other devices through interfaces such as the IEEE 1394. The combination of the basic

watermarking technology and adequate statistical processing over several frames provides a good solution to invisible video watermarking robust to MPEG-2 compression.

HOW IT WORKS

Any copyright mechanism consists of two main parts: copyright registration, and image protection. Through the registration procedure your image is uniquely identified and the time of registration is logged for later usage. In addition you can insert other copyright information, such as usage-rights and right-holder information. Upon registration a copyright certificate and a registration number, also called *IDDN number* will be issued . The second part, image protection, consists of inserting the IDD number into the image. This technology called digital watermarking inserts the IDD number by invisibly modifying the image. Image protection robustly links the IDD number to the image and allows for functionalities such as image tracking and monitoring. Moreover, due to the nature of the IDD number it allows the lawyers to make the evidence that you are the legal owner.

SOME IMPORTANT ISSUES

The transition from watermarking for still images to video sequences required several changes to the algorithm. The most prominent feature of video sequences is the increased sensitivity to changes introduced by the watermarking process. Even for parameter settings that minimize the watermark strength, watermarking artifacts are visible in high-quality digital beta cam video sequences.

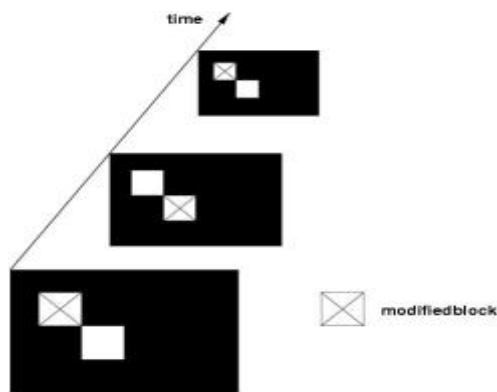


Figure 2.2: Visibility problem in consecutive frames(A).

Figure above illustrates the visibility problem. The block position is no longer restricted to a single image (x and y axes) but extends to the time axis, t. The modification of blocks that are close to each other in x and y as well as in t can result in flickering effects. To avoid such degradation, video streams must be processed more carefully than still images.

**Original****Marked****Checked & Marked**

Figure 2.3: Visibility problem in consecutive frames(B).

Homogenous areas within frames are particularly sensitive to this type of degradation as are regions containing sharp edges. Two criteria for checking blocks before actually embedding the watermark information have been introduced: **edge detection** and **plain area detection** mechanisms.

Figure shows DCT artifacts in edge and homogenous areas. The effects are exaggerated to make the problem visible using a still image. Figure (bottom left) shows the original clipped image; Figure (bottom center) shows the clip marked without the check algorithms. Here,

artifacts in both homogenous and edge regions are clearly visible. Figure (bottom right) shows the same part marked and checked for edge and homogenous blocks.

Edge detection

Numerous edge-detection algorithms are available, ranging from simple ones like the Sobel operator to more sophisticated ones, such as wavelet-based schemes. Because our algorithm aims at real-time capabilities, tools we use for edge detection must work fast. Even simple schemes like the Sobel operator have a computational complexity too high to be applied in real time. To minimize the overhead for edge detection, we use features computed within the basic algorithm cycle. The lowest frequency DCT coefficients of a transformed block can be used to decide whether the block contains an edge. The threshold value depends on the specific implementation of the DCT transform used.

Plain-area detection

The detection of smooth blocks is equivalent to a block's texture analysis. To avoid computational overhead, we use a criterion based on the block's quantized DCT coefficients. Instead of counting the number of non-zero coefficients in a transformed block's predefined region, as proposed by Benham et al., we look at the set of quantized coefficients selected for modifications. If one of the set's quantized coefficients equals zero, the block is classified as a "plain block".

Robustness against MPEG-2 encoding

Despite the transparency demands in watermarked video streams, the watermark must be robust against digital TV MPEG-2 encoding. The watermark information must survive MPEG-2 encoding, which is applied immediately before transmission. Two features of the MPEG-2 standard are very important (and challenging) for watermarking algorithms:

- The MPEG-2 encoder is very effective at removing spatial and temporal redundancy from the video stream.

- The MPEG-2 encoder keeps the video stream data rate constant. The data are compressed as much as needed to reach this goal. In rare cases, the encoder will skip complete frames.

The algorithm developed by the Security Technology for Graphics and Communication Systems department at the Fraunhofer Institute for Computer Graphics for watermarking and monitoring video streams in a TV-broadcasting environment survives MPEG-2 compression of high-quality, real-world video sequences without degrading their quality. The algorithm was designed with real-time applications in mind and has been successfully implemented in hardware, yielding a real-time marking and monitoring mechanism for high quality video signals.

EXPLORING CDMA FOR DIGITAL VIDEO WATERMARKING

INTRODUCTION

Digital video is paradoxically a simpler and more difficult medium to watermark than still imagery. Video by its nature is a wideband high bit-rate data carrying complex and dynamic information in the scene. Although complex watermark embedding and extraction procedures may be practical for a single image, the same cannot be said for video due to the sheer volume of data. For the same reason, it is more difficult to tamper with or completely eradicate a video embedded watermark. Even a short segment of video contains hundreds of frames, increasing the chance that the embedded watermark remains unscathed. Also, wideband nature of the data provides additional capacity for the placement of watermarks with large information contents such as video-in-video applications.

The appeal of spread spectrum in watermarking is understandable. Spread spectrum is in many ways a secure data-hiding algorithm and so is watermarking. Early examples of SS watermarking goes back to van Schynold who perturbed the LSB of each pixel by random amounts produced by an m -sequence generator. Cox definition of spread spectrum was rather different. They applied perturbation to the first 1000 largest DCT coefficients of the entire image. The perturbations were drawn from a normal random number generator. The choice of DCT coefficients was further refined to take into account the visual masking of human visual system. Smith and Comiskey framed watermarking as a modulation problem

and adopted the direct sequence spread spectrum model. The closest work to the present paper is that of Hartung and Girod. They have proposed a CDMA-style approach to video watermarking by first spreading a binary watermark by an m -sequence. Video frames are then rasterized and the spread watermark is added, pixel-by-pixel, to produce the watermarked video.

In this project I am presenting a framework for large scale watermarking of multimedia databases of uncompressed digital video using the formalism of CDMA. Here I will illustrate that video, as a time-space function, is a natural candidate for application of direct sequence spread spectrum. In particular, CDMA format, by virtue of its multiuser structure, is particularly suitable for a centralized effort for source or destination-based watermarking of large multimedia database titles.

CDMA AND ITS RELEVANCE TO WATERMARKING

CDMA is an application of direct sequence spread spectrum. The purpose is to combine multiple signals that overlap in both time and frequency yet remain separable. The separability is achieved by first projecting individual messages onto near-orthogonal PN sequences prior to carrier modulation. The number of simultaneous users in the system dictates the choice of a particular sequence. Maximal length, Kasami and Gold sequences have widely been used in practice for different reasons. For example, m -sequences provide the longest period, but do not offer as many orthogonal choices as do the other two. The application of CDMA to watermarking seems obvious. The goal is to watermark a large multimedia database using near-orthogonal watermarks. For example, a single title may receive user specific, individualized and near-orthogonal, watermarks. It is then possible to implement a watermark based search of the database to identify to whom that particular title was sold. The question is to what extent the traditional formulation of a CDMA signal carries over to watermarking. To place the problem in the proper context, we first briefly review the basic components of a CDMA signal below. The k th message is characterized by a bitstream $b_k(t) \in \{-1, +1\}$, with bit length Tb . $b_k(t)$ is then projected onto a PN sequence of pulses with amplitude $a_j^{(k)} \in \{-1, 1\}$ and chip length Tc such that $Tc/Tb = N$. This operation results in a bandwidth expansion factor or processing gain of N . Above can be summarized in the following expression

$$\begin{aligned}
a_k(t) &= \sum_j a_j^{(k)} p(t - jT_c) \text{ spreading sequence} \\
b_k(t) &= \pm 1, 0 \leq t \leq T_b, a_j^{(k)} = \pm 1, 0 \leq t \leq T_c, \frac{T_b}{T_c} = N \\
p(t) &= \begin{cases} 1, & 0 \leq t \leq T_c \\ 0 & \end{cases} \\
s_k(t) &= b_k(t) a_k(t) \text{ DS/SS signal}
\end{aligned}$$

Eq. 1

The complex envelope of the composite CDMA signal in the presence of phase and timing uncertainties is given by

$$s(t, \tau, \theta) = \sum_{k=1}^K a_k(t - \tau_k) b_k(t - \tau_k) e^{j\theta_k} + n(t)$$

Eq. 2

The receiver, in its simplest form consists of K banks of correlators where each bank correlates $s(t, \tau, \theta)$ with $a_k(t)$ over one bit interval. Since there are N chips in one bit, the resulting processing gain provides the well known protection against interference. This property is achieved at the cost of an N -fold increase in bandwidth. Presence of phase uncertainties, timing errors and partial correlation among the spreading codes cause cross couplings among various branches of the correlator bank.

The essence of CDMA is the concealment of message sequences by noise-like cover signals. In the context of watermarking, video is not the message, the watermark is. Video simply acts as the cover image. This is the opposite of the conventional CDMA where the cover image is in effect the pseudorandom sequence and is of no value to the end user. Another difference is that the conventional CDMA signal bears no useful information for the end user unless the signal is despread and the message recovered. In the context of watermarking, the message, i.e. watermark, is of no value to the end user per se. In fact, the existence of a “receiver” is not even necessary for information delivery. As such, CDMA, if used as is, is more a cryptographic operation and not a steganographic one.

Despite the differences outlined above, CDMA provides a well understood framework for watermarking of large multimedia databases. We will demonstrate, however, that watermarking brings its own unique requirements to the table. Therefore, many of the conventional aspects of CDMA will have to be modified, expanded or done away with altogether.

DEVELOPMENT OF CDMA WATERMARKING MODEL

There are several prior references to CDMA watermarking of digital video. Hartung and Girod's work is notable in recognizing CDMA as a viable choice for video watermarking. Their approach parses the video into a linear stream of individual pixel elements. A watermark represented by a binary pattern is then expanded by an m -sequence and added pixel-by-pixel to the uncompressed video. Watermark recovery is done by matched filtering. Instead of linearizing the video as a 1-D pixel stream, we model the video as a *bitplane* stream; the 2D counterpart of bitstream used in (1). By closely following the conventional CDMA model, it is possible to address a variety of watermark removal/destruction attempts that go beyond random noise attacks. For example, any spread spectrum watermarking that relies on m -sequences is extremely sensitive to timing errors. Frame drops, intentional or otherwise, destroy the delicate pattern of an m -sequence and can seriously challenge watermark identification.

We model digital video as a function in time and space represented by $I(x, y, t)$. $I(x, y, t)$ can then be sequenced along the time axis as bitplanes:

$$I(x, y, t) = \sum_j \sum_{n=0}^b i(x, y, t - (jT_f + nT_b))$$

Eq. 3

where $i(\cdot)$ is the n th bitplane of the j th frame positioned at $t = jT_f + nT_b$. T_f and T_b are frame length and bitplane spacing respectively and are related by $T = bT_b$ where b is the number of bitplanes per frame.

Two questions arise at this point, 1): how is a watermark defined? and 2): where in the bitplane stream is it inserted?. We define the watermark by a bitplane, $w(x, y)$, spatial dimensions of which match that of the

video frames. The content of the watermark plane can be selected to suite varied requirements. It can contain a graphical seal, textual information about the source or any other data deemed appropriate for watermarking. In the context of CDMA, $w(x, y)$ can be thought of as the message. This message is then spread using a 2D m -sequence or m -frames $\phi(x, y, t)$. To generate m -frames, a one dimensional m -sequence is rearranged in a 2D pattern. Depending on the period of the m -sequence and the size of each video frame, the 1D to 2D conversion may span up to k frames and will repeat afterwards. Spreading of the

“message”, i.e. the watermark $w(x,y)$ is now defined by a periodic frame sequence given by

$$w_{ss} = w(x,y) \sum_{j=0}^{k-1} \phi_j(x,y,t_j)$$

Eq. 4

where $\phi_j(x,y,t_j)$ is ϕ_j positioned at yet to be determined locations $t = t_j$. w_{ss} must now be aligned with and inserted into video bitplane stream in (3). The embedding algorithm works as follows. In every frame the bitplane at $t = t_j$ is tagged then removed and replaced by $\phi_j(x,y,t_j)$. The question now is which bitplanes are tagged and in what order? It is safe to assume that in most cases the LSB plane bit distribution is random and can be safely replaced by the watermark. However, LSB plane is vulnerable to noise and other disturbances but bitplanes can be used to embed a watermark with small to negligible effect on quality. In one example, watermark placement in one of 4 lower bitplanes did not significantly impact video quality.

In order to embed w_{ss} in the video, we define a separate multilevel sequence v and use $v(j)$ as pointer to the j th bitplane position. There are many ways to create v . One simple method is to start with a binary m -sequence u and add 3 cyclically shifted versions. Let $u = (u_0, u_1, \dots, u_{p-1})$ be an m -sequence of period p . Define D as an operator that cyclically shifts the elements of u to the left $D(u) = (u_1, \dots, u_{p-1}, u_0)$. We define v by $v = u + D(u) + D^2(u)$ where D^k is the k th cyclic shift of u . The new sequence now has two key properties, 1): it is still periodic with period p and 2): it is a 4 valued sequence taking on amplitudes in the range $\{0,1,\dots,3\}$. The significance of 4 values is that the watermark will be limited to 4 lower bitplane positions. This number can clearly change. We can now align w_{ss} in (4) with the timeline defined in (3)

$$w_{ss} = w(x,y) \sum_{j=0}^{k-1} \phi(x,y,v(j)T_b)$$

Eq. 5

w_{ss} is now a spread spectrum version of the watermark at pseudorandom locations determined by $v(j)$. The second task is accomplished by using $v(j)T_b$ as pointers to the candidate bitplanes where the watermark must be inserted. In order to take the last step, the

designated bitplanes must be removed and replaced by the corresponding elements of wss . The formalism to achieve this goal is through the use of a gate function defined by

$$gate(t - v(j)T_b) = \begin{cases} 0 & \text{for } t = v(j)T_b \\ 1 & \text{otherwise} \end{cases}$$

$$0 \leq t \leq T_f$$

Eq. 6

Multiplying video bitplane stream in (3) by the gate function above removes the bitplane at $v(j)$. The spread watermark bitplane stream in (5) is positioned such that the individual planes correspond exactly to the planes just nulled by the gate function. Putting it all together, CDMA watermarked video can be written as

$$I_{wm}(x, y, t) = \sum_j \left\{ \sum_{n=0}^{b-1} i(x, y, jT_f + nT_b) gate(t - jT_f - v(n)T_b) + w(x, y) \phi_j(x, y, jT_f + v(n)T_b) \right\}$$

$$\phi_{j+k} = \phi_j$$

Eq. 7

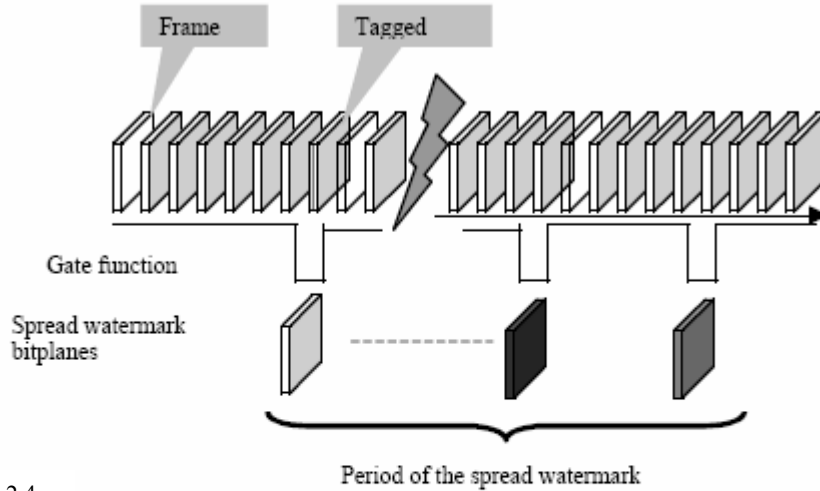


Figure 2.4

Graphical representation of CDMA video watermarking. Raw video is represented by a bitplane sequence. One bitplane per frame is pseudorandomly tagged over the length of video. In parallel, a 2D watermark is spread via a 2D m -sequence with period k . The tagged planes are then replaced by the spread watermark. The watermark is now hidden under two layers of security; 1): watermark location is pseudorandomly moved and 2): the watermark itself is spread via another PN sequence

ROBUSTNESS ISSUES : NOISE AND SYNCHRONIZATION

A successful watermark must meet at least two requirements; robustness and imperceptibility. In the context of video, watermark embedding algorithm must also be

simple and fast. It is showed that the lower 4 bitplanes are relatively safe for the placement of watermark. Moreover, a correlation receiver proved surprisingly resilient in recovering the watermark at SNR's as low as 5dB. This resiliency is achieved for two reasons. First, watermark is less vulnerable because its position is not limited to LSB, rather it moves pseudorandomly among a number of bitplane positions. Second, the processing gain provides significant protection against interference and noise. A CDMA-based watermarking, as a direct sequence spread spectrum, is extremely sensitive to timing errors, however Separating the desired watermark from others depends on the delicate auto and cross correlation properties of the underlying m -sequences which in turn depends on proper alignment of incoming and reference m -sequences.

A practical correlation-based watermark recovery must be able to operate asynchronously. In the present situation a chunk of video is extracted from the middle of a clip and decomposed into a bitplane sequence. The locations of spread watermark in the video are known from the multilevel sequence v in (5). Working with this information as well as the contents of watermark planes, a sliding correlator can easily pick out watermark planes despite possible initial timing offset. However, there are other more complex scenarios that a simple sliding correlator cannot handle. One possible scenario is frame drops. This situation arises in two causes, 1): an attempt at watermark removal may involve subsampling of the video. Subsampling can take place either at regular or random intervals and 2): frame drops may not necessarily occur out of malice. The recording process and other abnormalities may in fact result in random frame drops. The reason subsampling is a viable attack scenario is the high interframe correlation of raw video where frame skipping may in fact be tolerable.

To evaluate the impact of frame drops on the correlation detector, we consider two cases, 1):regular drops and 2): random drops. Recovering the embedded watermark from a subsampled video is equivalent to the problem of correlation of an m -sequence with a decimated version of itself. One nice property of all m -sequences is that if $u[q]$ is the decimated version of u by a factor of q , the inner product $\langle u, u[q] \rangle$ exhibits the same period as the original correlation $\langle u, u \rangle$. In other words, correlation still peaks and with the same period if the timing of the embedded watermark is disturbed. The same does not hold for random frame drops, however. First, there is the question of how often and where frame drops have occurred?. The answer depends on the period of v , w_{ss} and their relation to

frame drop rate. Assuming one drop per period of v , watermark extraction reduces to the correlation between the following two m -sequences:

$$\langle (v_0, v_1, \dots, v_{n-1}, v_n, v_{n+1}, \dots, v_{p-1}), (v_0, v_1, \dots, v_{n-1}, v_{n+1}, v_{n+2}, \dots, v_{p-1}, v_0) \rangle$$

Eq. 8

The second vector indicates that the n th frame has been dropped. This correlation consists of two partial correlations. The first part is the autocorrelation of v at lag 0 using only the first n out of p terms. The second term is partial correlation at lag 1 using the remaining terms. The magnitude of (8) is clearly less than $\langle v, v \rangle$. However, the residual correlation arising from partial correlation in (8) is still larger than cross correlation of v with v' where v' corresponds to a sequence used by a different user/watermark. As the n th dropped frame moves from the beginning to the end of the period, the magnitude of the above inner product increases.

WATERMARKING APPLICATIONS

- Proof of Ownership over an Image - "Robust" Watermarking: the detection of the mark with a private key or the hidden message itself helps in proving the ownership on a document.
- Monitoring of the Exploitation of Broadcast or Distributed Images: the notion of monitoring globally corresponds to tracing the distribution of some images on a given media of distribution. So, it concerns the evaluation of broadcast audience of a programme (also called: people metering) in a legal context, as well as the tracking of piracy (illegal exploitation) of some creations on a distribution media. But, its aim only remains detection of the exploitation of images.
- Fingerprinting: in order to complete the tracing of image exploitation on a distribution media, a different mark is inserted in each distributed copy of an image before delivery by its legal distributor. This identifies a transaction or a sold item.
- Document Integrity Checking - "Fragile" Watermarking: the mark permits to detect eventual changes in an image due to some attacks and their locations. Then, it is expected to be partly alterable.

- Authentication and Identification of an Image: a user which receives an image may need to identify the source of a document or the document itself with a high degree of certainty, in order to validate this document for a specific use.
- Usage Control: the reception of some distributed images by some digital equipment in a distribution network, may be controlled in using watermarks inserted in these images, and only enabled on equipment whose owner paid some access rights. A first example of it is provided Copy Protection on DVD & CDROM for the Consumer Market: a mark is embedded in DVD video disks in order to prevent copy of DVD, in co-operation with playback and recording devices manufacturers.
- Information Side Channel: this is globally related to "conveying" side information. About carrying public or private information, we generally think of information which is related to the image creation, and which is made available or not, to any receiver (depending on its nature). At the opposite, Steganography is concerned with secretly carrying information that has nothing to do with the "cover" image: this really constitutes a separate channel.

3. WATERMARKING EVERYTHING

The first watermarks for digital images were close imitations of paper watermarks. A watermark image is superimposed on the image to be protected. The watermark is only faintly visible, without disturbing the host image too much



Watermarks in Mark and Dollar bank notes

SCENARIO 1: You have produced a work of art, say an image. You want to publish this image in digital form. You embed an invisible watermark into the image. This mark should be very hard to remove without destroying the whole image. If somebody else claims ownership of your work you can use the watermark to prove that this is your work.

Another use of watermarks is *tamper proofing or image verification*. Here the aim is to prove that an image has not been changed in the least.

APPLICATIONS OF WATERMARKING

- ✚ **Give your images the power of personalization and protection:** Using this you can add a layer of protection to your images by identifying copyright ownership and delivering a tracking capability that monitors and reports where your images are being used. You can protect your images by tracking them beyond your own domain. This will increase control over your assets by tracking and reporting on their authorized and unauthorized use.
- ✚ **Limit unlicensed use:** Using this you can limit unlicensed use and receive information to help recover otherwise lost revenue.
- ✚ **For digital audio and video:** Similar to the process in which artist artistically signed their paintings with a brush to claim their copyrights; artists of today can watermark their work and hide for example their name in the image. Hence, the embedded watermark will allow identifying the owner of the

work. It is clear that this concept is also applicable to other media such as digital video and audio. Especially the distribution of digital audio over the Internet in the MP3 format is currently a big problem. In this scenario digital watermarking may be useful to set up a controlled audio distribution and provide efficient means for copyright protection.

- ✚ **Certification:** For example, in the field of data security, watermarks may be used for certification, authentication, and conditional access. Certification is an important issue for official documents, such as identity cards or passports.



- ✚ **To mutually linking information on the documents:** That means that some information is written twice on the document: for instance, the name of a passport owner is normally printed in clear text and is also hidden as an invisible watermark in the photo of the owner. If anyone would intend to counterfeit the passport by replacing the photo, it would be possible to detect the change by scanning the passport and verifying the name hidden in the photo does not match any more the name printed on the passport.
- ✚ **The authentication of image content:** The goal of this application is to detect alterations and modifications in an image. The three pictures below illustrate an example of this application. The picture on the left shows an original photo of a car that has been protected with a watermarking technology. In the center, the same picture is shown but with a small modification: the numbers on the license plate have been changed. The picture on the right shows the photo after running the watermark detection program on the tampered photo. The tampered areas are indicated in white and we can clearly see that the detected areas correspond to the modifications applied to the original photo.



(a)



(b)



(c)

✚ **Conditional access and copy-control:** For example conditional access to confidential data on CD-ROMs may be provided using digital watermarking technology. The concept consists of inserting a watermark into the CD label. In order to read and decrypt the data stored on the CD, the watermark has to be read since it contains information needed for decryption. If someone copies the CD, he will not be able to read the data in clear-text since he does not have the required watermark. The picture below shows an example of a protected CD. To read the data on the CD, the user starts a program on the CD. This program asks the user to put the CD on the scanner and then reads the watermark. If the watermark is valid the program decrypts the data on the CD and gives the user access the clear-text data. (Patent pending, contact us for license.)

✚ **Copy-control:** Several companies work on a watermarking system for copy control in the DVD environment. Fully functioning solutions exist already, however, for the moment they have not been entirely approved by the content producers and providers. Finally, this solution is also an efficient and simple way to prevent the use of illegal copies of software. It has a similar functionality as the anti-piracy device called "dongle", but is more compact and less expensive.

✚ **As invisible labels and content links :** For example, photo development laboratories may insert a watermark into the picture to link the print to its negative. This way is very simple to find the negative for a given print. All one has to do is scan the print and extracted the information about the negative. In a completely different scenario digital watermarks may be used as a geometrical reference which may be useful for programs such as optical character recognition (OCR) software. The embedded calibration watermark may improve the detection reliability of the OCR software since it allows the determination of translation, rotation, and scaling.

TYPES OF WATERMARK

✚ **SEMI-FRAGILE WATERMARK:** A semi-fragile watermark is a mark which is (highly) sensitive to a modification of the stego-medium. A fragile watermarking scheme should be able to detect any change in the signal and identify where it has taken place and possibly what the signal was before modification. It serves at proving the authenticity of a document.

✚ **ROBUST WATERMARK:** A robust watermark should be stuck to the document it has been embedded in, in such a way that any signal transform of reasonable strength cannot remove the

watermark. Hence a pirate willing to remove the watermark will not succeed unless they debase the document too much to be of commercial interest.

CLASSES OF WATERMARKING

- ✚ **PUBLIC OR BLIND WATERMARKING:** In these schemes, the cover that is the original signal is not needed during the detection process to detect the mark.. Solely the key, which is typically used to generate some random sequence used during the embedding process, is required
- ✚ **SEMI-BLIND WATERMARKING:** In some cases you need extra information to help your detector (in particular to synchronize its random sequence on the possibly distorted test signal). In particular some watermarking schemes require access to the 'published' watermarked signal, that is the original signal just after adding the watermark.
- ✚ **PRIVATE OR NON-BLIND WATERMARKING :** The original cover signal is required during the detection process.
- ✚ **ASYMMETRIC OR PUBLIC-KEY WATERMARKING :** In this case, the detection process (and in particular the detection key) is fully known to anyone as opposed to blind watermarking where a secret key is required. So here, only a 'public key' is needed for verification and a 'private key' (secret) is used for the embedding though. Knowledge of the public key does not help to compute the private key (at least in a reasonable time), it does not either allow removal of the mark nor it allows an attacker to forge a mark.

FEATURES OF WATERMARKS

An invisible watermark for copyright protection should be :

- ✚ **Hidden or Imperceptible :** The insertion of the watermark should not degrade the host signal. Also, the presence of the watermark should not be readily visible. This goal is in conflict with the next two.
- ✚ **Robust :** The watermark should resist manipulations which might occur in legitimate use : filtering, lossy compression, cropping , printing and scanning, conversion to a different data format, . Cox and Miller have argued that the watermark must be placed in perceptually significant regions of the host signal to resist lossy compression.
- ✚ **Tamper resistant :** The watermark should resist attempts to remove it. This is not an absolute requirement, rather it is linked to the level of degradation of the host signal. A “brute force “ attack which destroys the host signal might well remove the watermark.
- ✚ **Secure :** The watermarked image should not reveal any clues of the presence of the watermark, with respect to un-authorized detection, or (statistical) undetectability or unsuspecting (not the same as imperceptibility).

- ✚ **Public :** The method of watermarking should be known to the general public. Like in cryptography “security through obscurity” is not a valid concept. By keeping a watermarking method secret you remove it from the peer reviewing process and thus make it less secure.
- ✚ **Multiple watermarks :** It should be possible to insert multiple watermarks. The watermarks of all the originals used and the watermark of the creator of the collage should still be detectable.
- ✚ **Scalable :** It should be possible to use better versions of the same technique when more computing power becomes available. This corresponds to the use of bigger keys in cryptographic algorithms. On the other hand the watermark should still be tamper resistant in spite of more computing power.
- ✚ **Self-clocking / arbitrary re-entrant :** If only fragments of the host signal are available - ,e.g. after cropping or rotating a picture – the watermark can still be recovered.
- ✚ **Resistance to collusion attack :** If several images marked with different watermarks are “ averaged” the result should still be watermarked. This feature is needed in two situations : In fingerprinting, where the same image is watermarked differently for different customers, and in the watermarking of videos, where several similar frames could be averaged.

The watermark could be :

- A chosen string of bits
- An image
- A sequence of floating point numbers with certain properties.

KEY POINTS TO REMEMBER

- ✚ **Watermark detection** should also be possible in case small modifications have been applied to the marked media. Such modifications can be the result of intentional attacks in order to remove the mark or the result of coding schemes (e.g. lossy compression that is compression where there is some loss of quality) and errors during the transmission. A robust watermarking scheme will be able to retrieve the watermark from this distorted media.
- ✚ **Watermark is embedded in only luminance components rather than in chroma components as well in image/video:** It has more to do with the survivability of the marked areas within an image. Color can easily be changed or converted to grayscale and you still have a "useable" image. In marking an image, one wants to place the mark in the more robust areas of an image. Areas of high luminance are not the correct assessment, because a plain sky may have high luminance but a poor structure for hiding information. What the watermark tools are really interested in are areas with high gradient magnitude. In other words, relatively strong edges with respect to the structure of the image and the luminance variances of the "edges."

A lot of watermarking schemes hide data in the luminance/intensity due to the fact that the Human Visual System (HVS) use most of its bandwidth on perceiving (changes in) brightness. In changing an image, by e.g. JPEG compression, one therefore has to be more gentle to the brightness information than to the color information (hue/saturation) since small changes in lightness might be easily detectable than large changes in color. If the compression changes the brightness in an image, this will give the outcome a poor quality to the HVS, and that is why these changes are avoided. For the watermark to be robust to e.g. compression, the watermark has to be in parts of the image that will not be changed in the compression. That is a reason why hiding data in the Luminance is a good idea.

In 1997 it was suggested to use the blue channel to embed a spread spectrum based watermark into an image. The blue channel was used because the HVS is less sensitive to blue colors due to the fact that the blue cones (S-cones) are less densely distributed than the green and red cones (M-, L-cones) in the foveal part of the human retina. Since then, we made numerous subjective tests and found that in average the energy of a blue channel watermark is up to 50 times larger than the energy of a luminance watermark, of course both introducing visually equivalent artifacts. This implies that the blue channel watermark is more robust towards attacks such as filtering (averaging, median, ...) and additive noise. Furthermore, we found that under lossy JPEG compression both approaches are approximately equivalent. However, one problem that goes with blue channel watermarks is that it is more difficult to control, or predict, the artifacts. That is, the visibility of a luminance watermark is more homogeneous and less dependent on the image colors. Therefore, the design of blue (or any other color) channel watermarks is more delicate and requires sophisticated models of the HVS to optimally adapt the watermark to the local contrast, intensity, and color. For instance, the attacker takes a coarse estimate of the power density spectrum of an image (very coarse: low pass characteristic), designs the Wiener filter accordingly, and perhaps can remove at least some of the watermark components (e.g., high pass watermark components). Note that the theoretical analysis described above confirms in an analytical fashion the heuristic argument given very early by Cox et al.



The watermark should be embedded into the most significant data components: Therefore, you should be very careful when designing your watermark based on psycho-acoustic or psycho-visual masking effects. If you put your watermark underneath a masking threshold, an attacker can remove it without any penalty. This approach is not the right one for very robust watermarks. Nevertheless, masking might be appropriate when embedding information just as added value (in this scenario we do not have a malicious attacker). Note that any state-of-the-art compression scheme (for audio and images) will significantly impair the watermark underneath the masking threshold.

✚ The theoretical analysis also gives you an idea about the **maximum information that can be embedded per pixel**. Assume that a mean-squared error distortion measurement is used. Further, let the attacker add simple additive white Gaussian noise (AWGN). In this case, Shannon's result for the capacity of an AWGN channel gives the upper limit on the achievable watermark rate, e.g. 0.5 bit/sample if the variance of the AWGN equals the embedding distortion. Everybody can play this attack! Thus, you never can achieve higher rates. Of course, more sophisticated attacks can be invented. Thus, in practice the achievable watermark rate will be much lower. The goal of current research efforts is to tighten this bound. Of course, tight bounds can be obtained only when optimizing the watermarking scheme and the attack for certain signals statistics. An "all-white" image has less (exactly zero) watermark capacity than a Gaussian-noise image (Moulin's result).

4. LITERATURE REVIEW

The Spread-spectrum is a transmission technique in which a pseudo-noise code, independent of the information data, is employed as a modulation waveform to “Spread” the signal energy over a bandwidth much greater than the signal information bandwidth. At the receiver the signal is “de-spread” using a synchronized replica of the pseudo-noise code.

BASIC PRINCIPLE OF SPREAD SPECTRUM

Direct Sequence Spread Spectrum

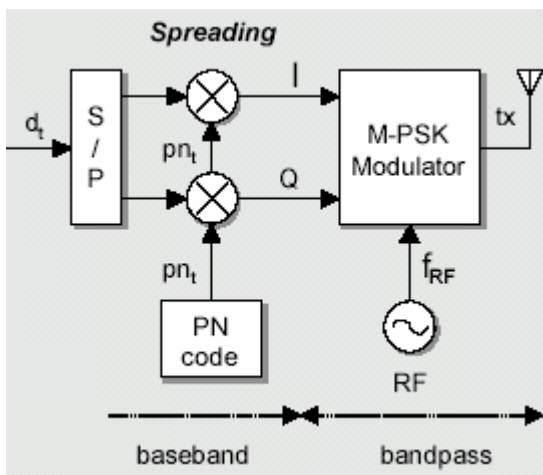


Figure 3.1 Modulator

A Pseudo-noise sequence p_{n_t} generated at the modulator (refer to fig. 2.1.1), is used in conjunction with an M-ary PSK modulation to shift the phase of the PSK signal Pseudo randomly, at the chipping rate $R_c (=1/T_c)$ a rate that is an integer multiple of the symbol rate $R_s (=1/T_s)$.

The transmitted bandwidth is determined by the chip-rate and by the base-band filtering. The implementation limits the maximum chip-rate(R_c) and thus the maximum spreading.

The PSK modulation scheme requires a coherent demodulation.

A short-code system uses a PN code length equal to a data symbol. A long code system uses a PN code-length that is much longer than the data symbol, so that a different chip pattern is associated with each symbol.

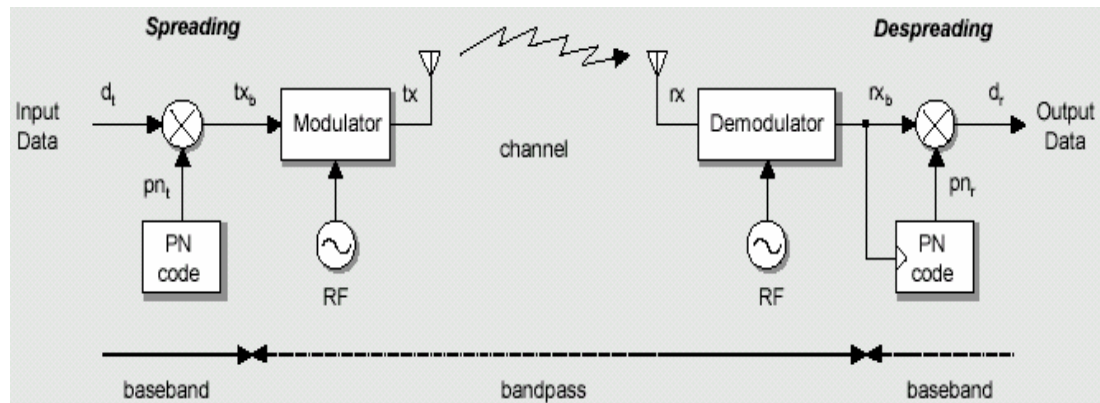


Figure 3.2 Building blocks of a DSSS system for BPSK Modulation

Spreading

In the transmitter, the binary data d_t (for BPSK, I & Q for QPSK) is ‘directly’ multiplied with the PN sequence pn_t , which is independent of the binary data, to produce the transmitted base-band signal tx_b .

$$tx_b = d_t \cdot pn_t$$

The effect of multiplication of d_t with a PN sequence is to spread the base-band bandwidth R_s of d_t to a base-band bandwidth of R_c .

De-spreading

The spread-spectrum signal can’t be detected by a conventional narrow-band receiver. In the receiver, the received base-band signal rx_b is multiplied with the PN sequence pn_r .

- If $pn_r = pn_t$ and synchronized to the PN sequence in the received data, then the recovery binary data is produced on d_r . The effect of multiplication of the spread-spectrum signal rx_b with the PN sequence pn_t used in the transmitter is to de-spread the bandwidth of rx_b to R_s .

- If $pn_r \neq pn_t$, then there is no spreading action. The d_r has a spread-spectrum. A receiver not knowing the PN sequence of the transmitter can't reproduce the transmitted data.

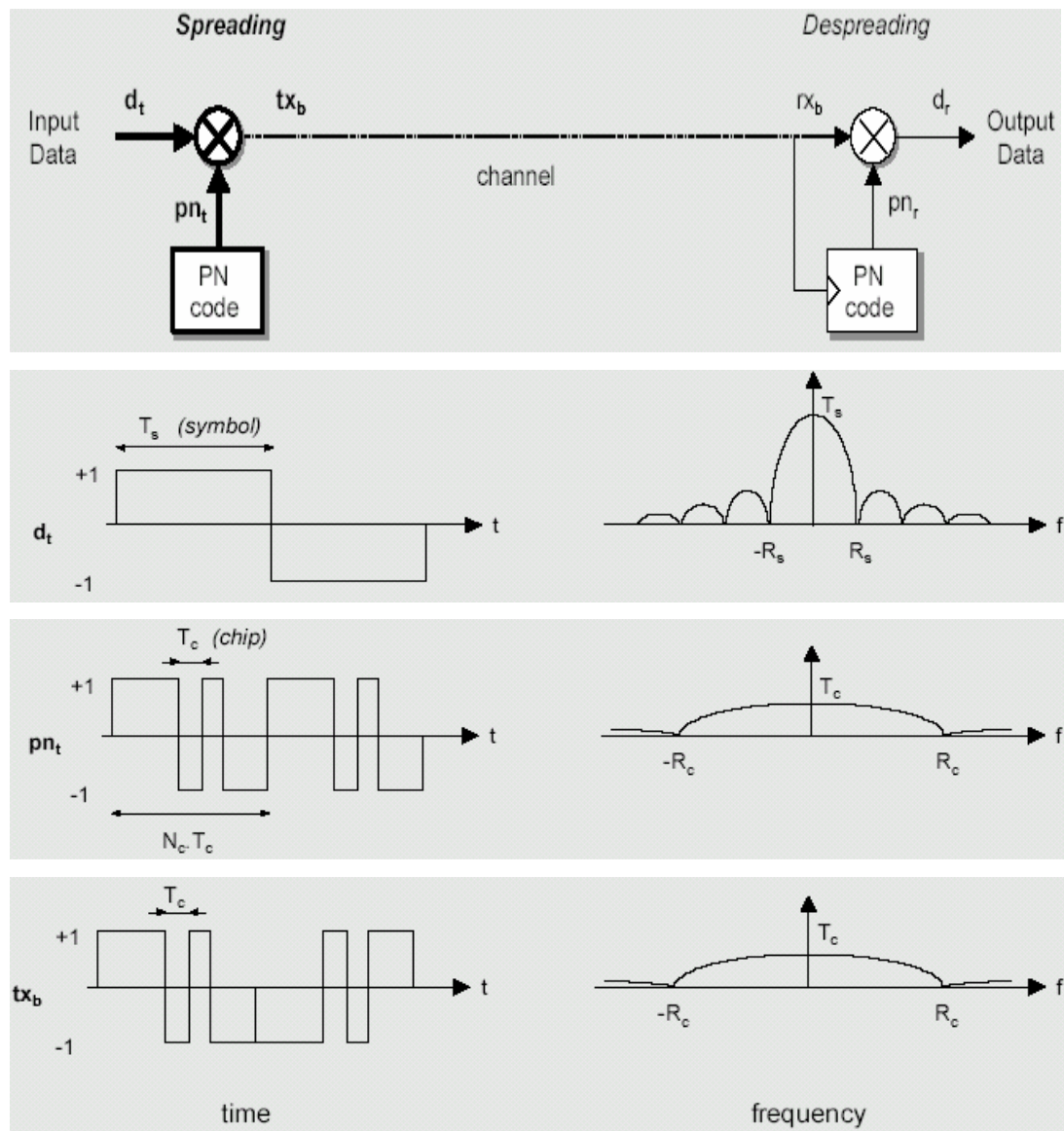


Figure 3.3 Spread –spectrum technique

Spread-spectrum systems are spreading the information signal d_t which has a BW_{info} over much larger bandwidth BW_{ss} :

$$BW_{info} \approx R_s \ll BW_{ss} \approx R_c$$

The SS-signal spectrum is white noise like. The amplitude and thus the power in the SS-signal tx_b is the same as in the original information signal d_t . Due to the increased bandwidth of the SS-signal, the power spectral density must be lower. The bandwidth expansion factor, being the ratio of the chip-rate R_c and the data symbol rate R_s is usually selected to be an integer in practical SS systems.

$$SF = G_p = BW_{ss}/BW_{info} = R_c/R_s = T_b/T_c = N_c$$

De-spreading

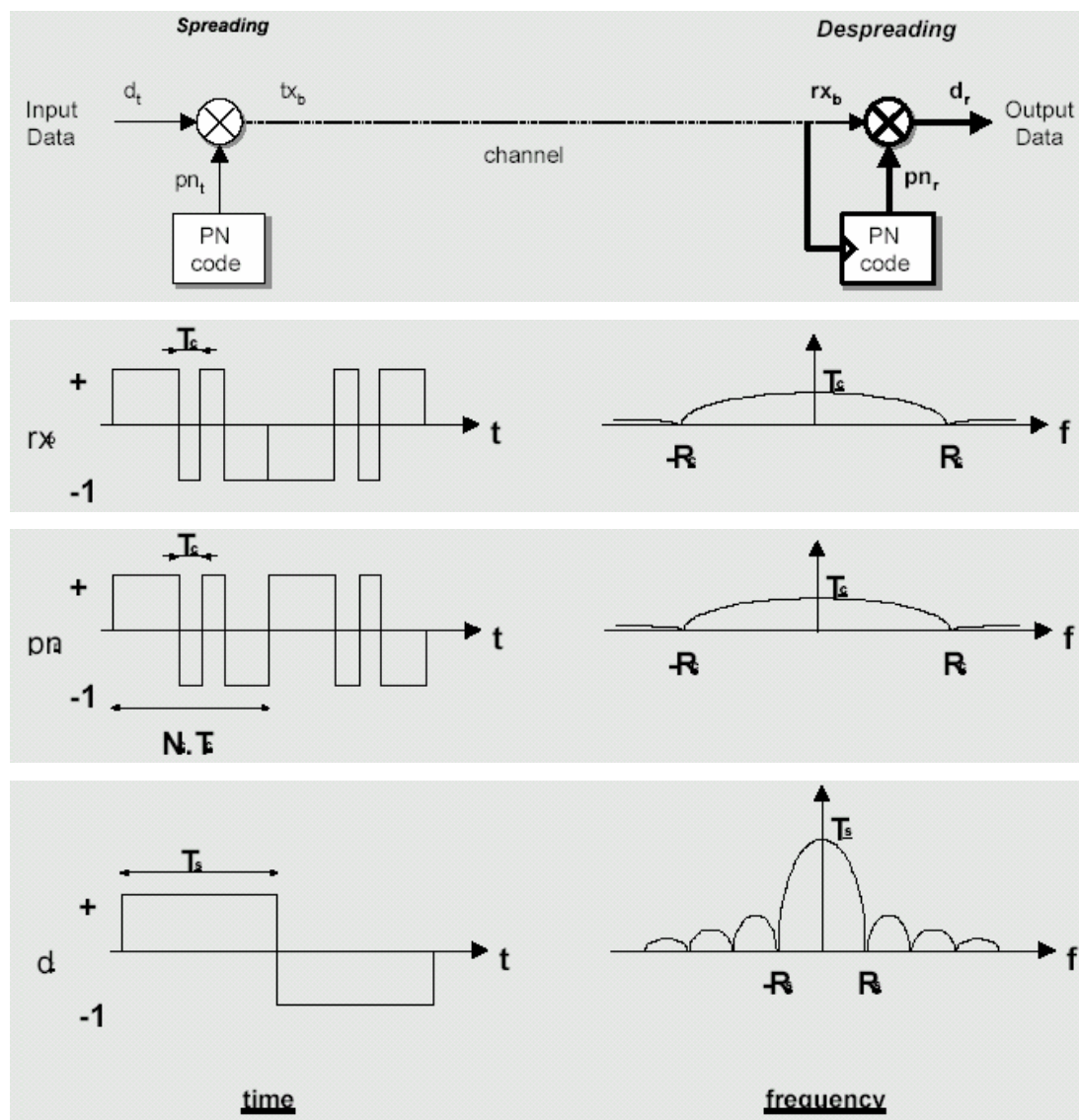


Figure 3.4 De-spreading technique

To demodulate, the received signal is multiplied by pn_r , this is the same PN sequence as pn_t , synchronized to PN sequence in the received signal rx_b . This

operation is called de-spreading. since the effect is to undo the spreading operation at the transmitter. The receiver output is:

$$d_r = r_{xb}.pn_r = (d_t.pn_t).pn_r \text{ where } pn_t.pn_t = +1 \text{ for all } t$$

Thus,

$$d_r = d_t$$

If the received signal is multiplied by PN sequence pn_r , different from the one used in modulator, the multiplier output becomes:

$$d_r = r_{xb}.pn_r = (d_t.pn_t).pn_r$$

Thus, for secure communication in a multi-user environment the transmitted data d_t may not be recovered by a user that doesn't know the PN sequence pn_t used at the transmitter.

PSEUDO-RANDOM NOISE

A pseudo – noise(PN) code sequence acts as a noise like(but deterministic) carrier used for bandwidth spreading of the signal energy. The selection of a good code is important, because the PN code sequence is a pseudo noise or pseudo - random sequence of 1's & 0's, but not a real random sequence(because periodic). Random signals can't be predicted. The auto-correlation of a PN code has properties similar to those of white noise.

Pseudo-Random

- Not random, but it looks randomly for the user who doesn't know the code.
- Deterministic, periodic signal that is known to both the transmitter & the receiver. The longer the period of the PN spreading code, the closer will the transmitted signal be a truly random binary wave , and the harder it is to detect.
- Statistical properties of sampled White noise

Code Length

- **Short code** : The same PN sequence for each data symbol($N_c.T_c = T_s$)

- **Long code :** The PN sequence period is much longer than the data symbol , so that a different chip pattern is associated with each symbol ($N_c.T_c \gg T_s$)

PROPERTIES OF SPREAD SPECTRUM

The following properties of spread spectrum are particularly well-suited for watermarking.

- ✚ **Anti – jamming :** The anti – jamming property results from the fact that an attacker does not know the privileged information that the sender and an authorized receiver possess. As a result, the attacker must jam the entire spectrum of the broadband signal. The jammer has limited power, however, so it can only jam each frequency with low power. Hence, the sender and the receiver have an effective signal-to-jammer advantage (called the processing gain).

With application to watermarking, the anti-jamming property means that, in order to jam a watermark, an attacker must distort the marked media severely – so severely that the attacker media is no longer of acceptable quality or has no commercial value.

- ✚ **Low probability of intercept :** The low probability of intercept property is a consequence of spreading : a large signal power is distributed over the entire frequency spectrum, so only a small amount of power is added at each frequency. Often, the increase is below the noise floor, so an attacker may not even detect the transmission of a spread-spectrum signal. This allows a watermark to be embedded unobtrusively.

- ✚ **Pseudo-noise :** For security, the carrier is often a pseudo-noise signal, meaning that it has statistical properties similar to those of a truly random signal, but it can be exactly regenerated with knowledge of privileged information. For example, the carrier could be the output of a random-number generator that has been initialized with a particular seed, and the seed is known only to the owner.

The pseudo-noise property is useful for watermarking, because it makes it difficult for an attacker to estimate the watermark from marked media. In addition, with properly chosen pseudo-noise signals, even if the attacker can perfectly estimate

some small segments of the watermark, it is not possible to determine the rest of the mark.

The low- and mid-frequency components of the image data represent most of the perceptual important information. Therefore, compression schemes and other image processing operations can hardly affect this significant portion of the host image without destroying much of the visual content of the image. Thus, adding the watermark in significant coefficients of the transform domain generally improves robustness. Spatial domain watermarking methods have to indirectly model the low-frequency component of the host image signal, which can be quite complicated to achieve.

In the DCT domain, the energy concentrates in the low frequency regions around the upper-left corner. The multi-resolution DWT representation has the low-frequency of the image signal in the approximation sub-band, also located in the upper-left corner, while the high-frequency components are represented in the detail sub-bands at several resolutions. Most energy of the detail sub-bands is situated in edge areas and textured regions.

The main disadvantages of the frequency transform domain techniques are their *computational cost*, and, in the case of a global transform, their *problem to adapt the watermark strength to the local image activity*, making it more difficult to exploit certain characteristics of the HVS system such as masking effects. The later shortcoming can be resolved by using the wavelet transform which provides frequency and spatial information of the host image.

5 THE WATERMARKING OF DIGITAL VIDEO

OBJECTIVE OF THE PROJECT

The Objective of the project is to ultimately embed a robust Watermark in the digital Video that will identify its Owner unambiguously.

- Initially a model of Watermarking system will be constructed.
- Further stages will demonstrate the use of CDMA technique for video watermarking using MATLAB.
- Objective also includes the study of various attacks e.g. compression, loss of synchronization on the watermarked video.

OVERVIEW OF THE PROJECT

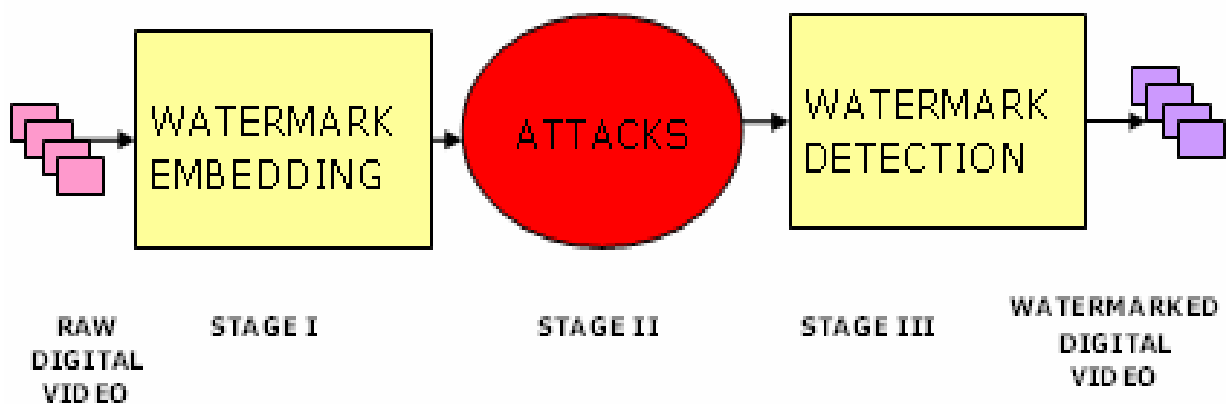


Figure 5.1 Watermarking Model

PROBLEM : I am proposing a technique for the watermarking of Digital Video. Recent attempts have been mostly focused on still image Watermarking. The Watermarked Video must be robust to Video editing attempts such as subsampling, Frame reordering etc. The Watermark should also be identifiable from arbitrary segments of Video. Individual frames extracted from the Video must also contain copyright information.

APPROACH : Digital Video possesses a component not present in still imagery : time. I will first develop a model for the Video signal and then proceed a formal extension of Direct Sequence Spread Spectrum in the form of m-frames. Watermarking is performed at bitplane level.

MODEL : First, Video signal is modeled as a sequence of bitplanes arranged along the third dimension ; time. Watermarking of this sequence is a two layer operation. A controlling m-sequence first picks candidate bitplanes for watermarking.. Watermark, defined as m-frames, supplants the tagged bitplanes. It will be shown that the watermark, when limited to the 4 lowest bitplanes, are unnoticeable. Moreover, attempts in corrupting the image to destroy the watermark renders the video useless before damaging the seal itself. The Watermarked Video is also robust to video editing attempts such as subsampling, frame reordering etc. the Watermark is also identifiable from arbitrary short segments of video. Individual frames extracted from the Video will also contain copyright information.

Among the most popular approaches the one used quite often are the Spread spectrum techniques. These approaches, however, do not meet the strict definition of a spread spectrum signal because the spectrum is really never spread. The linkage with spread spectrum is only in the use of m-sequences to modify specific DCT blocks of the image.

The problem of Watermarking of digital video has received considerably less work. In its simplest interpretation, video watermarking may be interpreted as watermarking of thousands of individual still frames. This extension, however, does not take into account interframe information flow as well as computational demands in the encoding and decoding phases. The forces that are expected to be exerted on the watermark are also different. Watermark in still images needs to be robust to geometric transformation such as recensing, rotation, translation, etc. These factors do not all carry over. For example, concerns over geometric transformations are clearly less applicable to Video than to still imagery. Watermarks designed for video need to have additional capabilities. For example, it may be required to trace one or several frames extracted from a video clip back to its original owner. It is also desirable to identify the watermark of an extended video from a very short observation interval starting at a random location.

In the following I present a Video watermarking scheme with several unique characteristics. The approach is founded on the principal of Direct Sequence Spread Spectrum with an extension to two dimensions. Watermarks are applied at bit plane levels, not casually

accessible, selected by an m – sequence. We then introduce the concept of m – planes, a 2-D extension of an m -sequence, to define the Video Watermark. A maximum likelihood detector can then recover the watermark from a very short observation interval down to a single frame.

A SIGNAL MODEL FOR VIDEO :

A T second video can be modeled by a stack of N frames separated in time by $T_f = T/N$. Each frame in turn can be represented by the sum of b bitplanes with $T_b = T_f/b$.

The signal model describes video as a sequence of individual bit planes separated in time by T_b . There are two main questions to be answered at this point,

- 1) which frame get the watermark and
- 2) what is the watermark?

Operating at the bit plane level, candidate planes for watermarking are picked based on markers defined by the ‘1’ positions of an m -sequence.

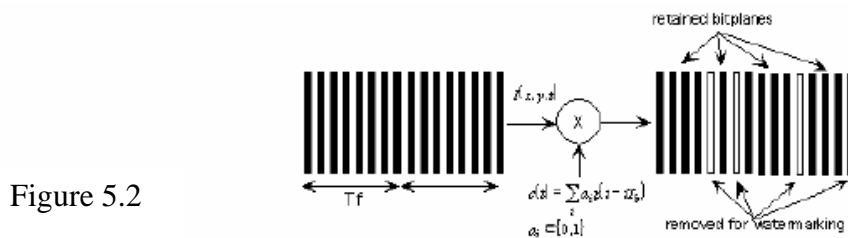


Figure 5.2

Video is modeled by a stream of bit planes. Watermarks are inserted as complete frames in random positions determined by an m -sequence not related to the watermarking scheme itself.

Here the tagged bit planes have been replaced by the spreaded watermarked planes result in some processing gain. Another point is the information displaced by the watermark is not put back in at the time of decoding. This is always an option but requires a decoder on the user's side.

Bit plane orders retained for watermarking have a direct impact on the visibility of watermark. Low bit orders are less visible but more susceptible to noise. Higher bit planes affect image quality more but are less affected by noise. The controlling m -sequence can be modified to limit watermarking to, say, k least significant bit planes.

STAGE 1: WATERMARK INSERTION

MODEL OF THE STAGE

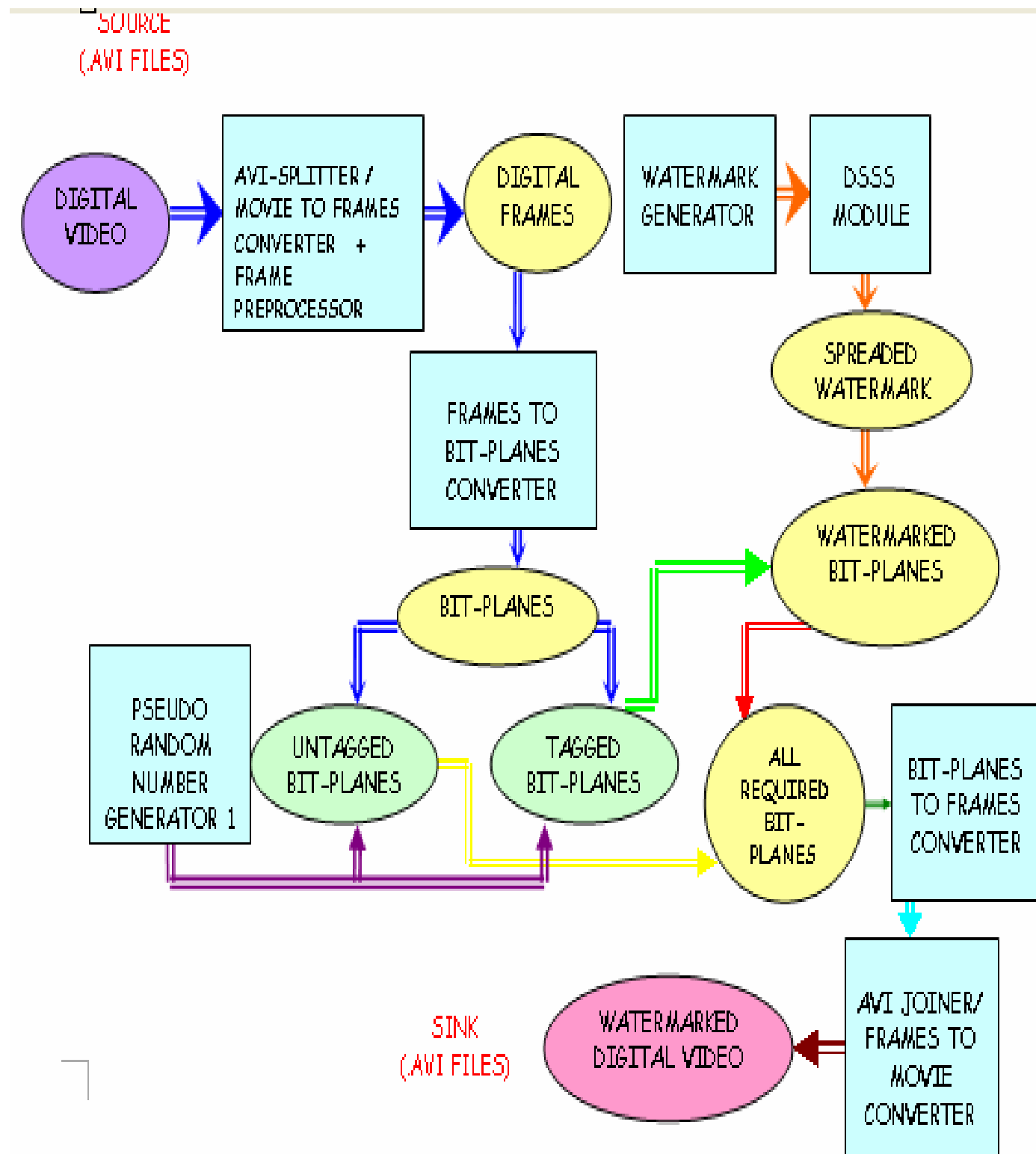


Figure 5.3 Complete Model of the digital Video watermarking

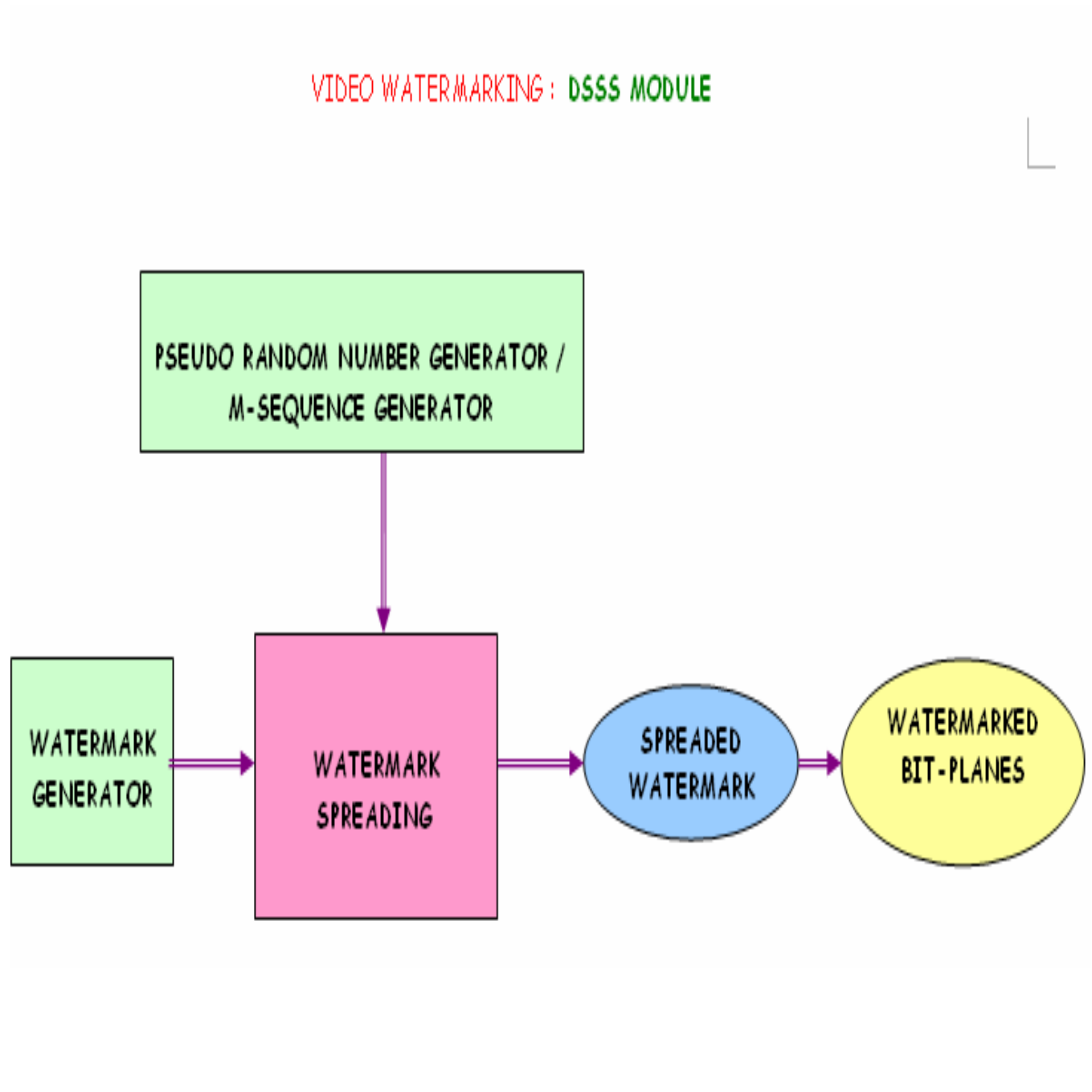
DIRECT SEQUENCE SPREAD SPECTRUM MODULE

Figure 5.4 Direct Sequence Spread Spectrum Module

WORKING OF THE STAGE

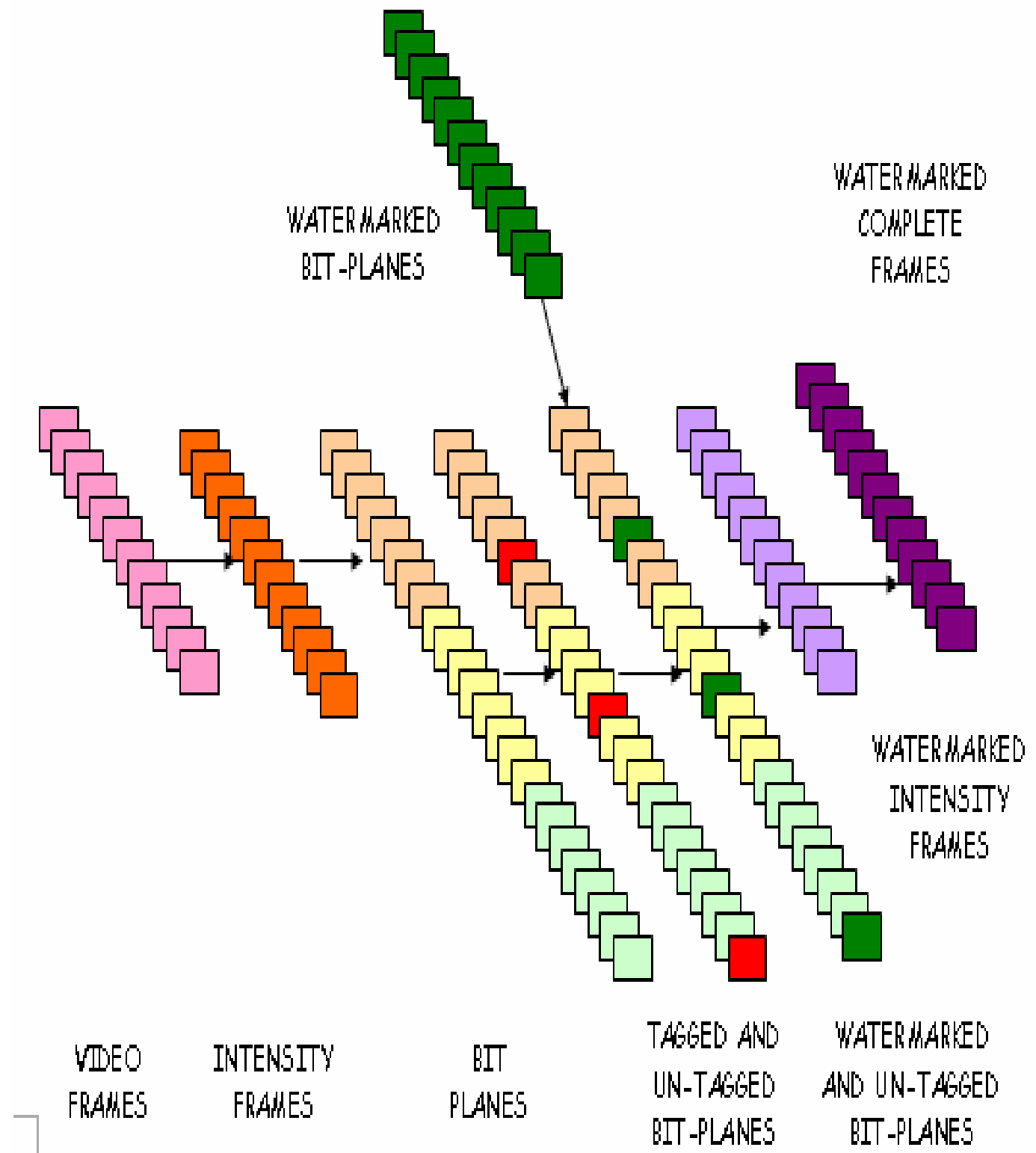
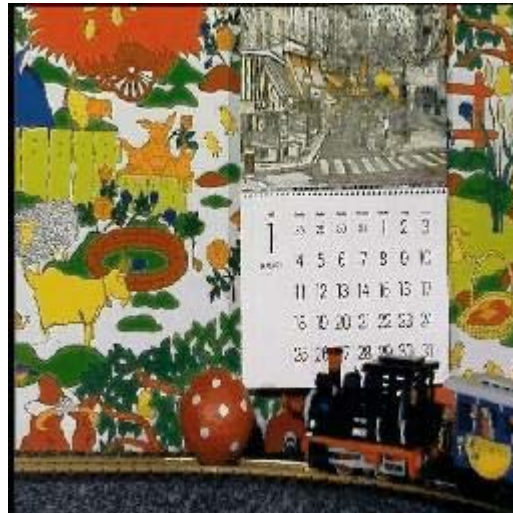


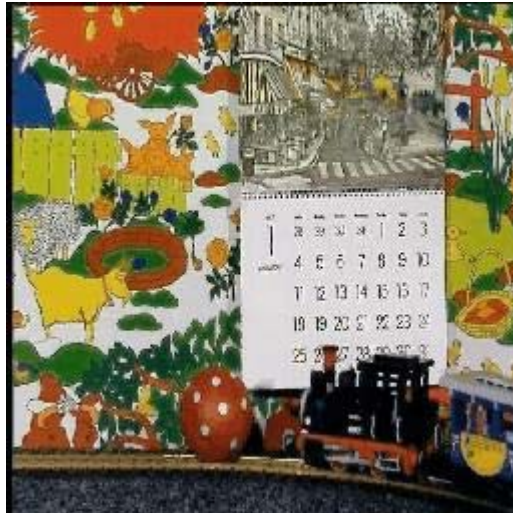
Figure 5.5

Working of the Stage I

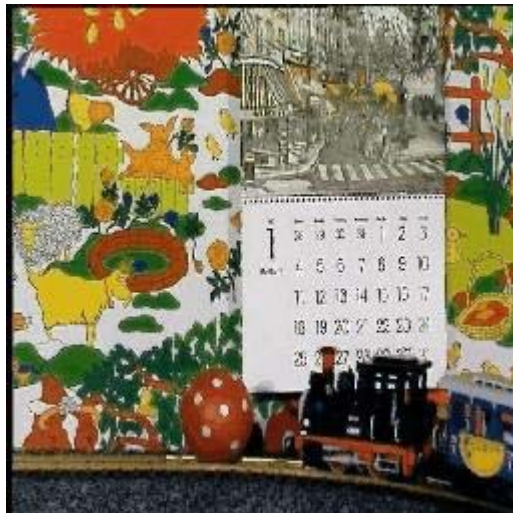
STEPS TO BE UNDERTAKEN

- ❖ Study theory of CDMA in detail.
- ❖ Study digital Video processing and Video Watermarking in details
- ❖ Study of pseudo-random noise (PN) sequences.
- ❖ MATLAB implementation of the WATERMARKING SYSTEM.

MATLAB CODE SIMULATION RESULTS**ORIGINAL FRAMES OF THE MOVIE****1. FRAME 1****2. FRAME 2****3. FRAME 3**



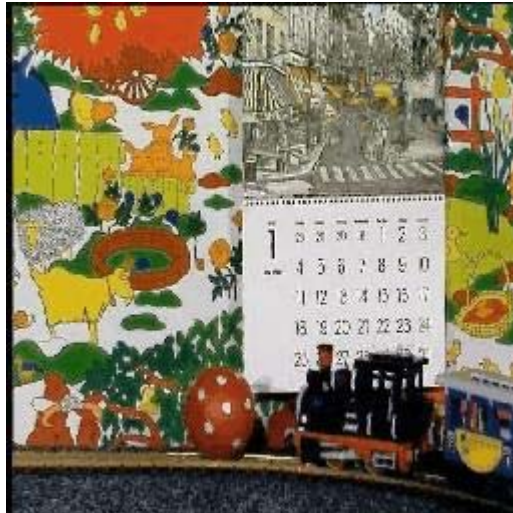
4. FRAME 4



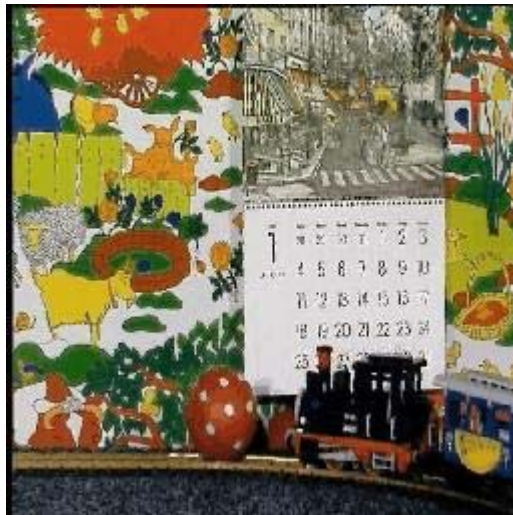
5. FRAME 5



6. FRAME 6



7. FRAME 7



8. FRAME 8



9. FRAME 9



10. FRAME 10



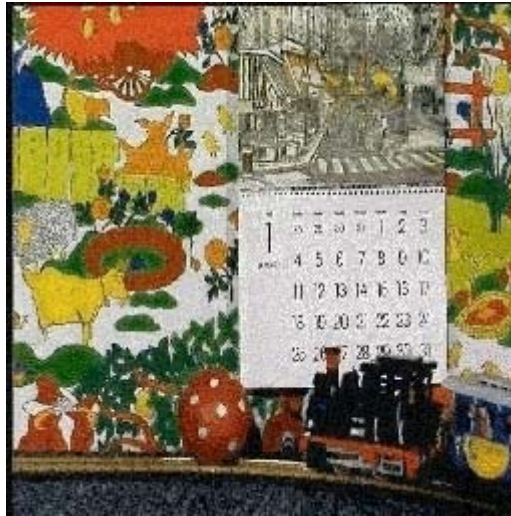
ORIGINAL WATERMARK USED

MONICA
GUPTA

WATERMARKED FRAMES

WATERMARKED MOVIE FRAMES (WATERMARKING MSB PLANES)

1. FRAME 1



2. FRAME 2



3. FRAME 3



4. FRAME 4



5. FRAME 5



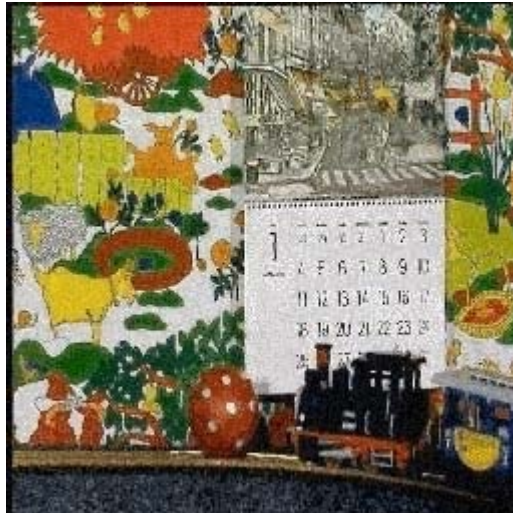
6. FRAME 6



7. FRAME 7



8. FRAME 8



9. FRAME 9

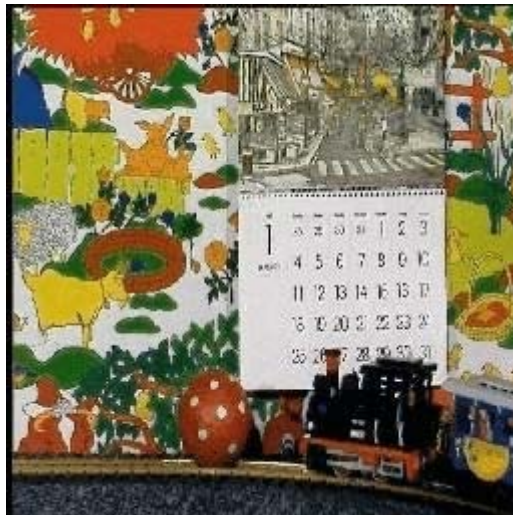


10. FRAME 10

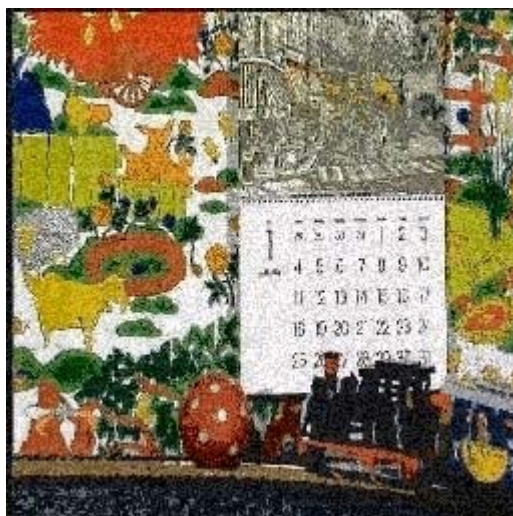


WATERMARKED MOVIE FRAMES (WATERMARKING MID-SB PLANES)

1. FRAME 1



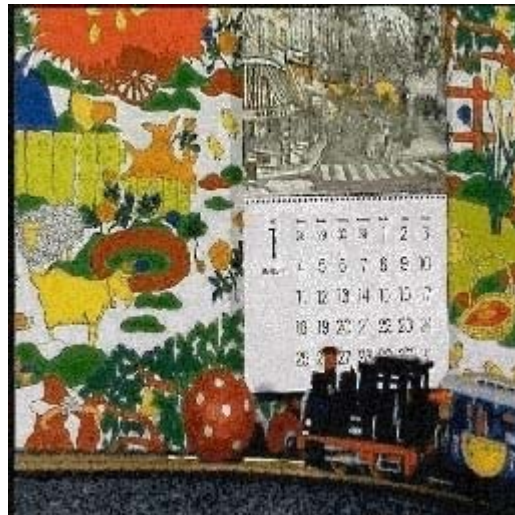
2. FRAME 2



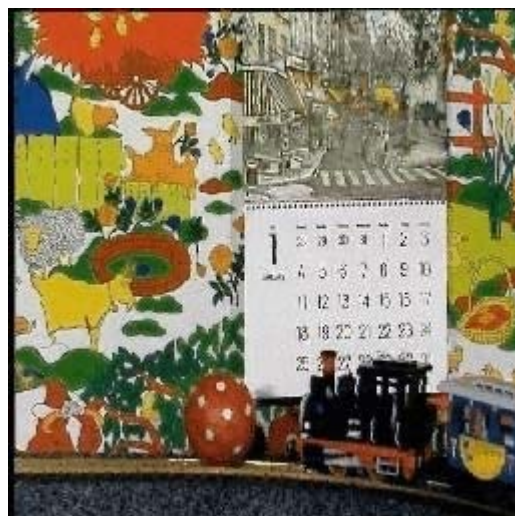
3. FRAME 3



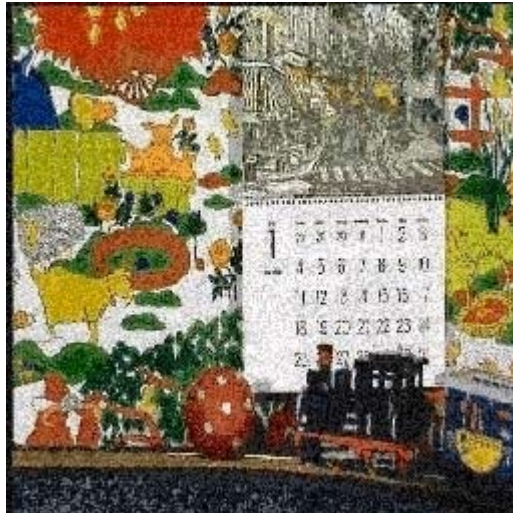
4. FRAME 4



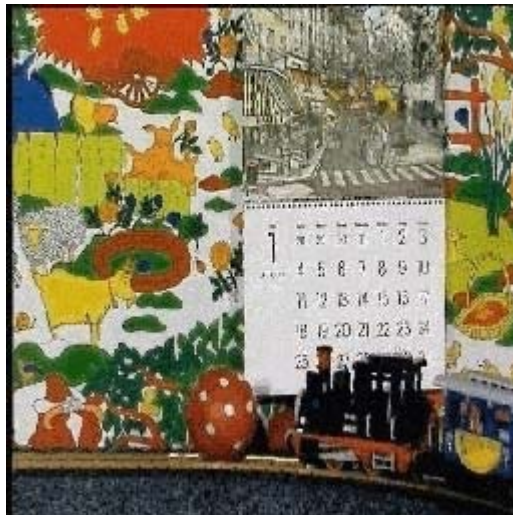
5. FRAME 5



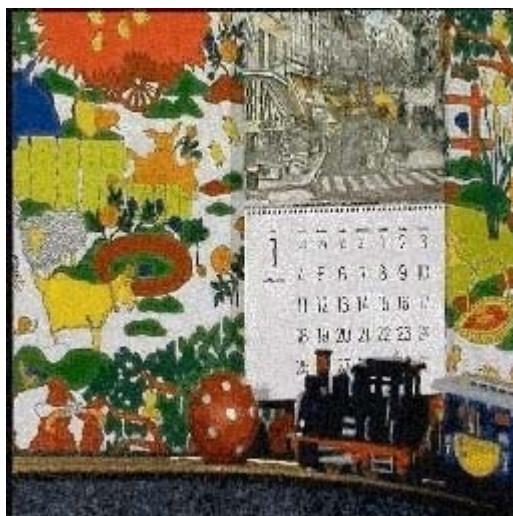
6. FRAME 6



7. FRAME 7



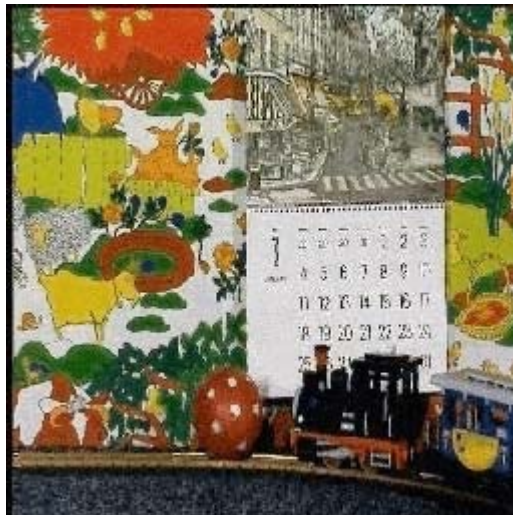
8. FRAME 8



9. FRAME 9

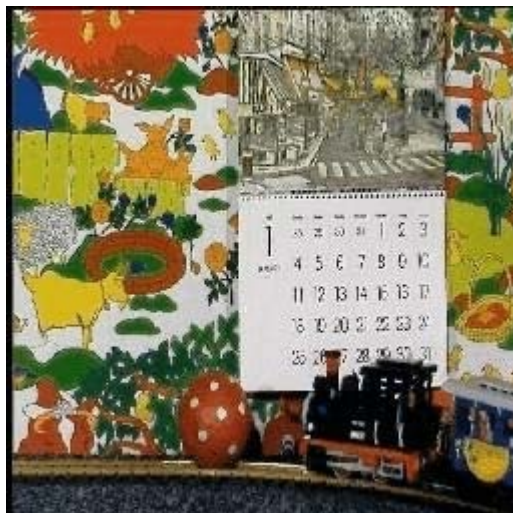


10. FRAME 10

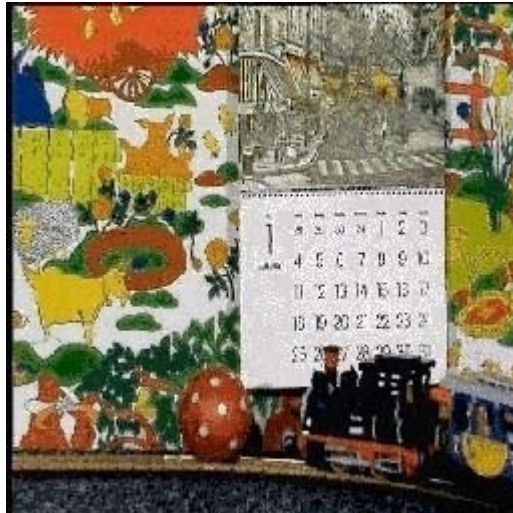


WATERMARKED MOVIE FRAMES (WATERMARKING LSB PLANES)

1. FRAME 1



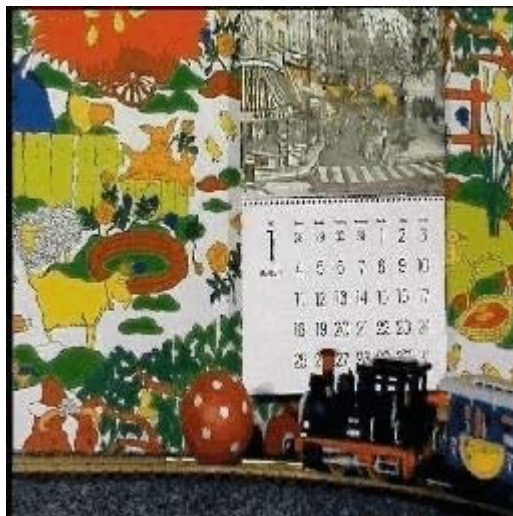
2. FRAME 2



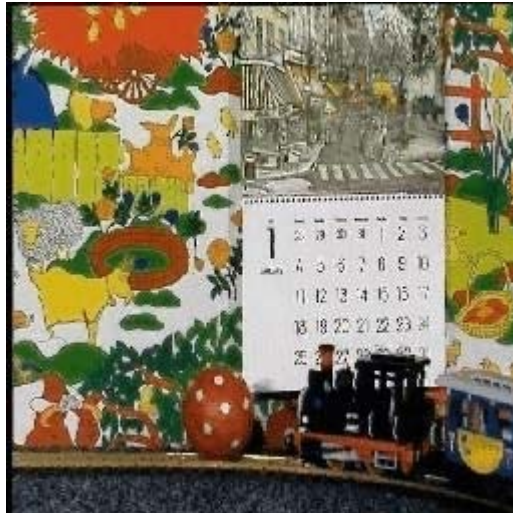
3. FRAME 3



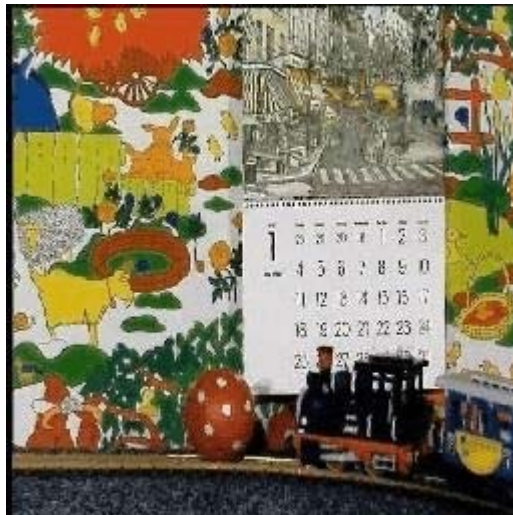
4. FRAME 4



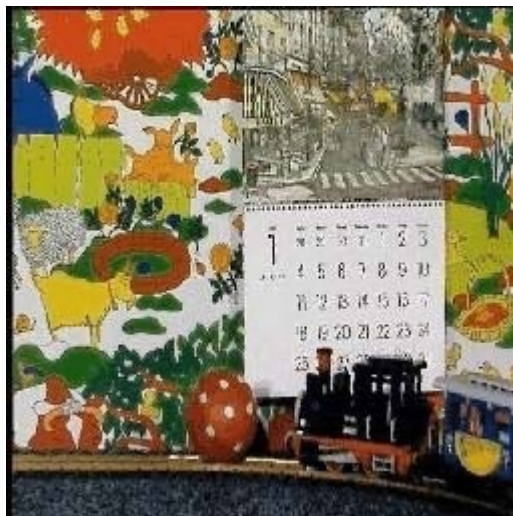
5. FRAME 5



6. FRAME 6



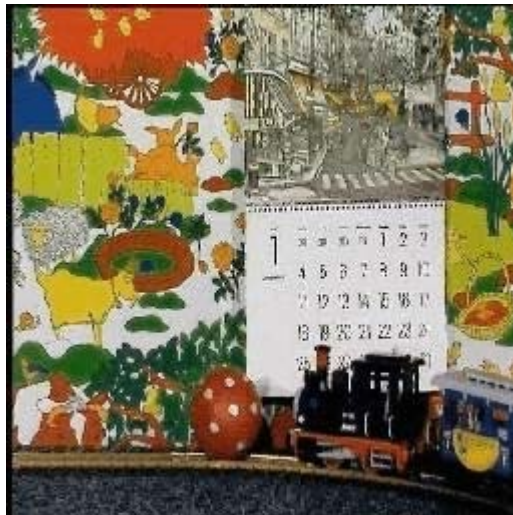
7. FRAME 7



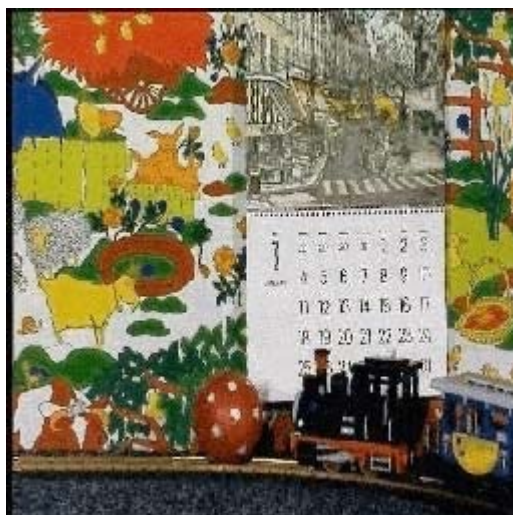
8. FRAME 8



9. FRAME 9



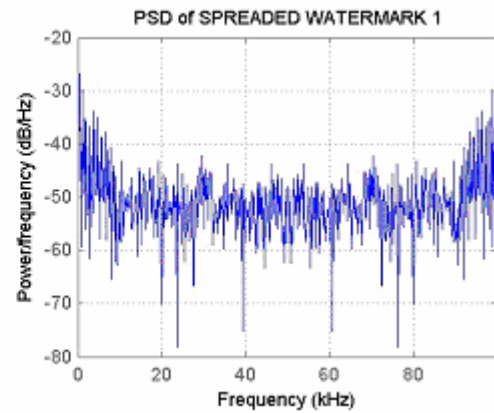
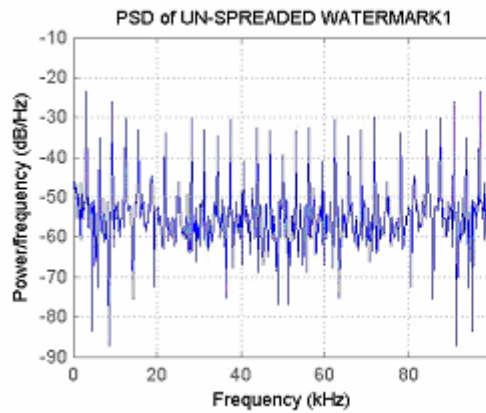
10. FRAME 10



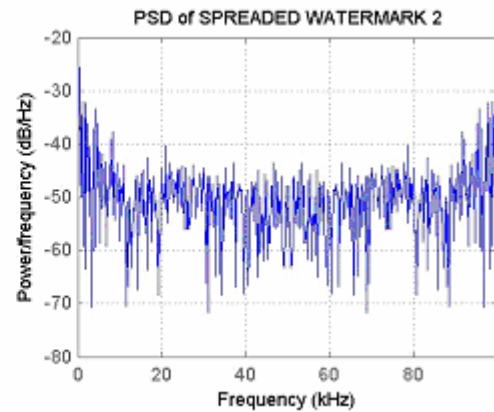
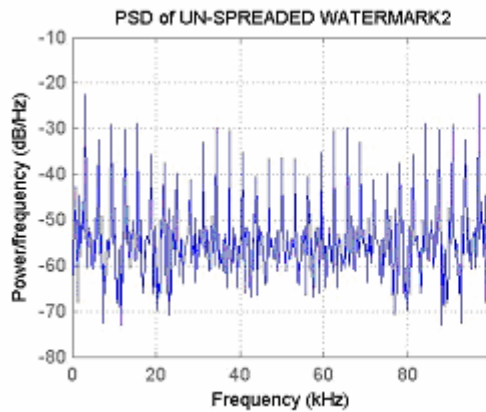
PERIDODGRAMS

PERIODOGRAM DISPLAY (WATERMARKING MSB PLANES)

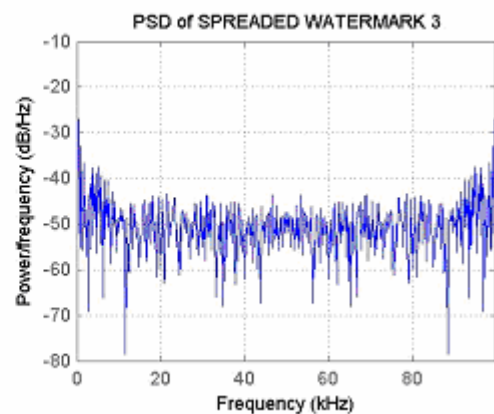
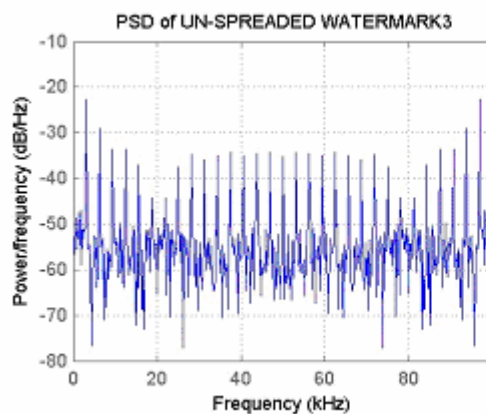
1. FRAME 1



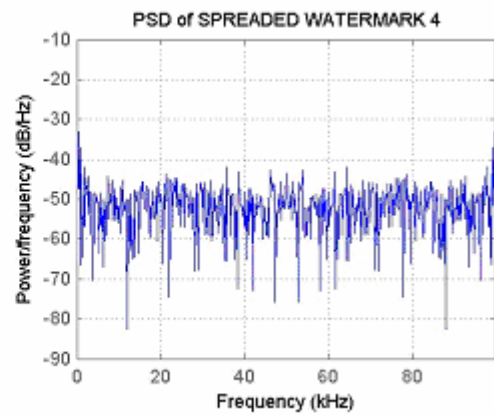
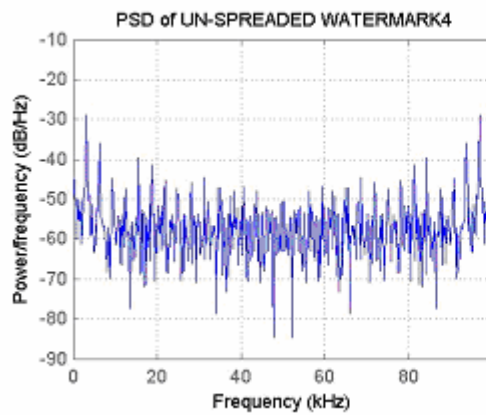
2. FRAME 2



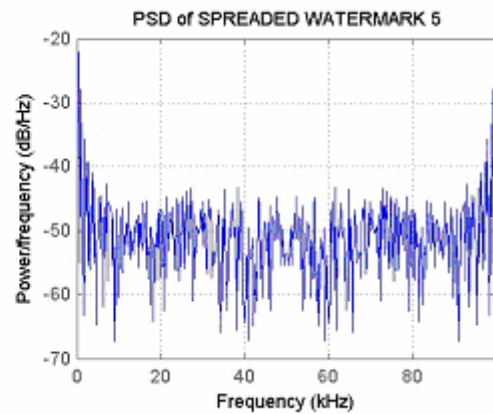
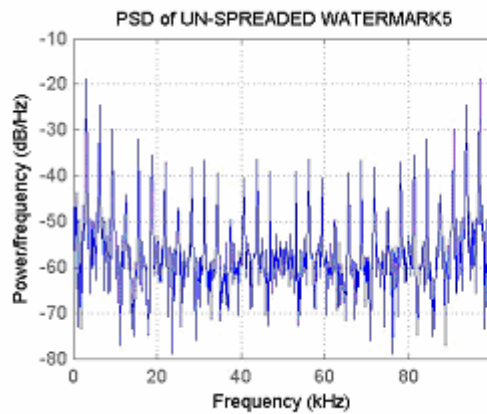
3. FRAME 3



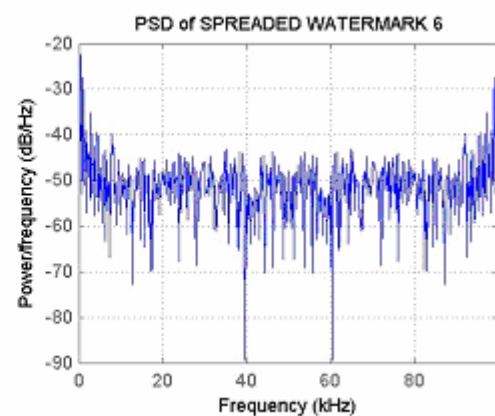
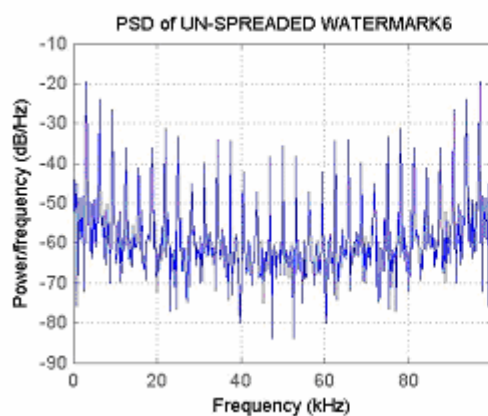
4. FRAME 4



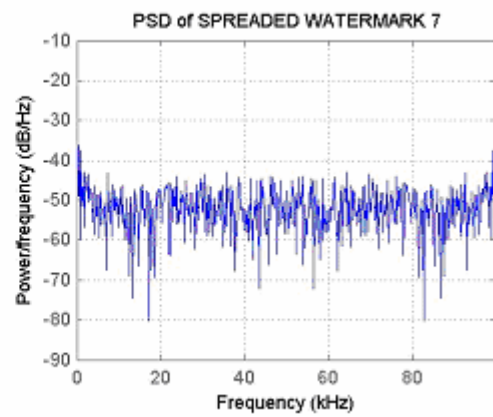
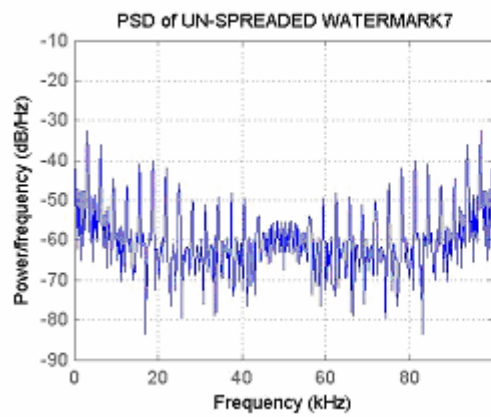
5. FRAME 5



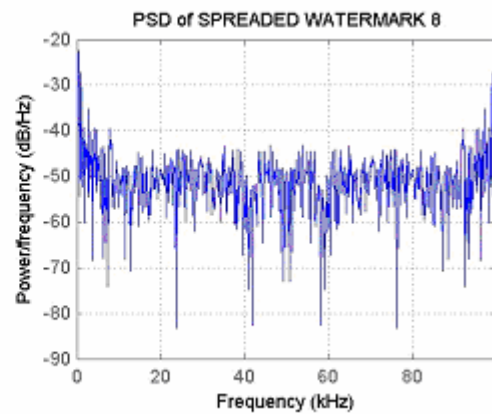
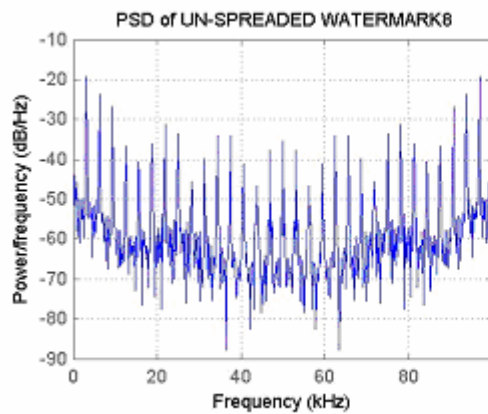
6. FRAME 6



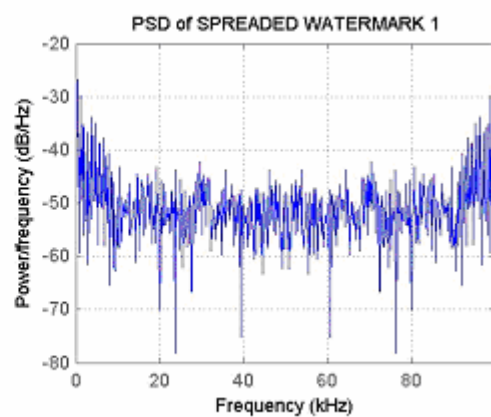
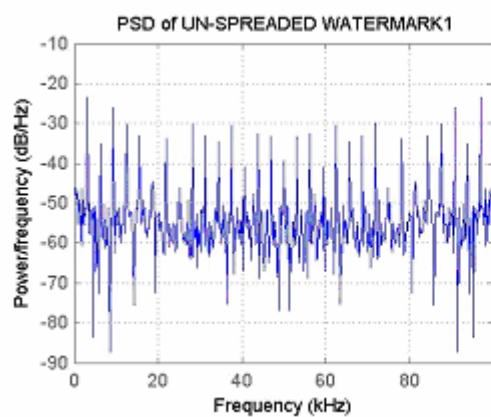
7. FRAME 7



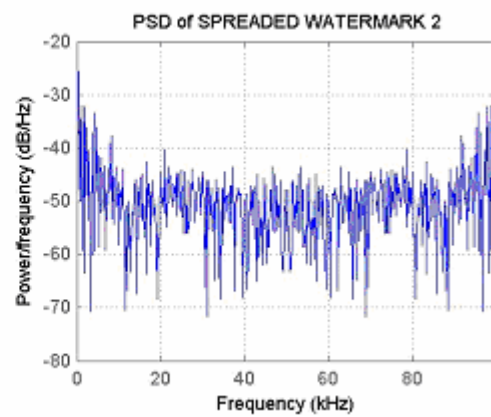
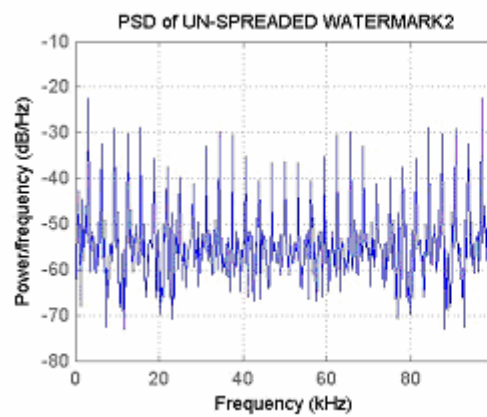
8. FRAME 8



9. FRAME 9

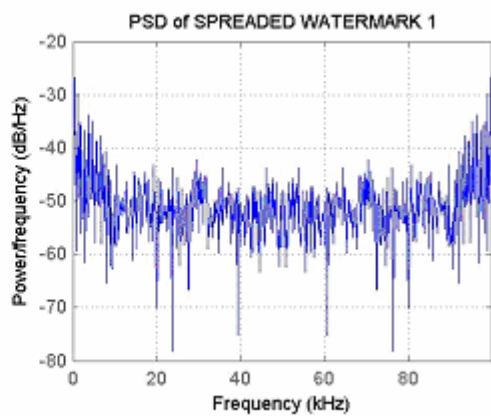
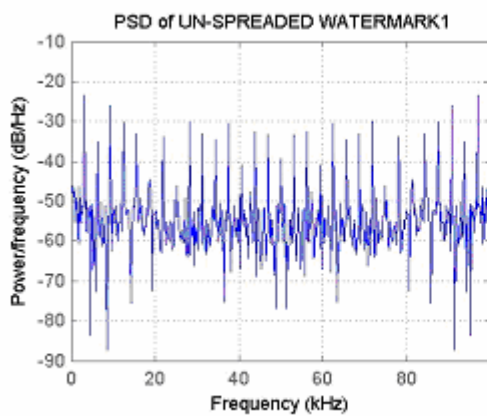


10. FRAME 10

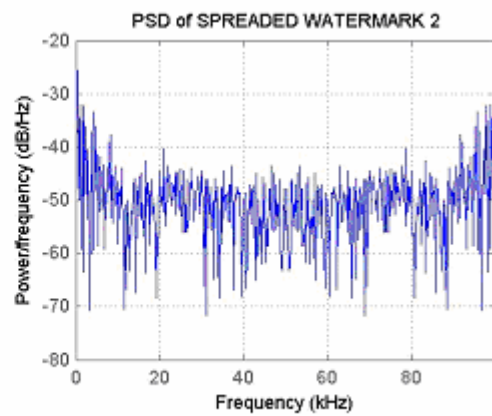
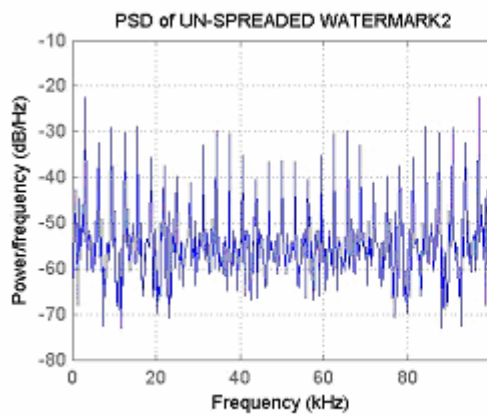


PERIDODOGRAM DISPLAY (WATERMARKING MID-SB PLANES)

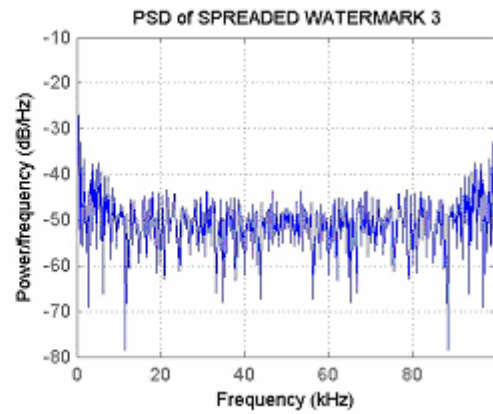
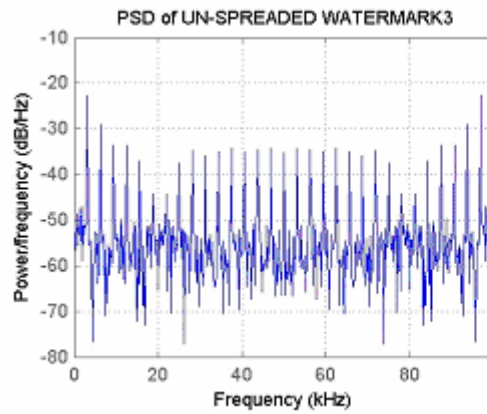
1. FRAME 1



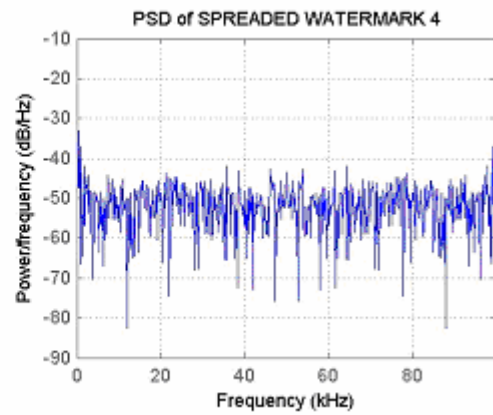
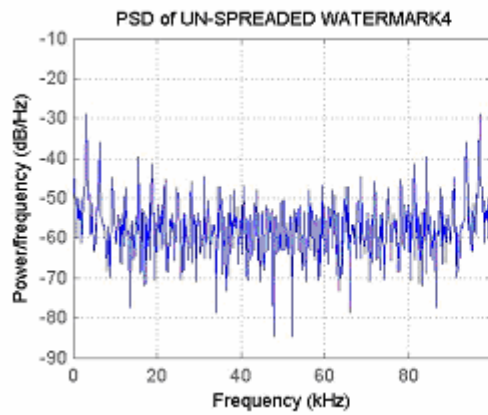
2. FRAME 2



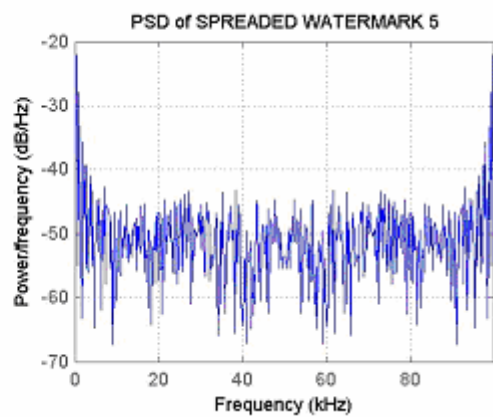
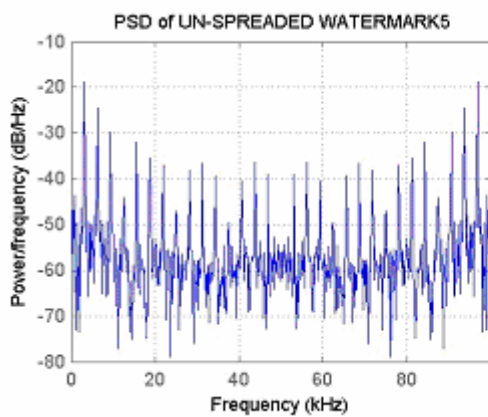
3. FRAME 3



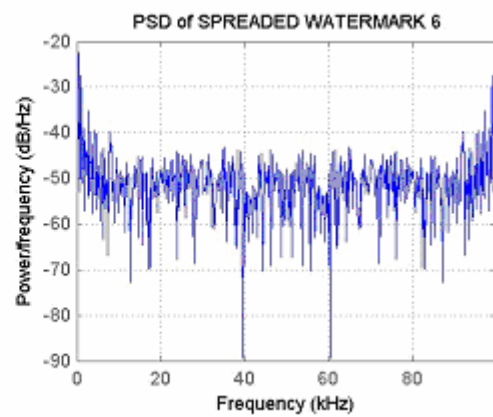
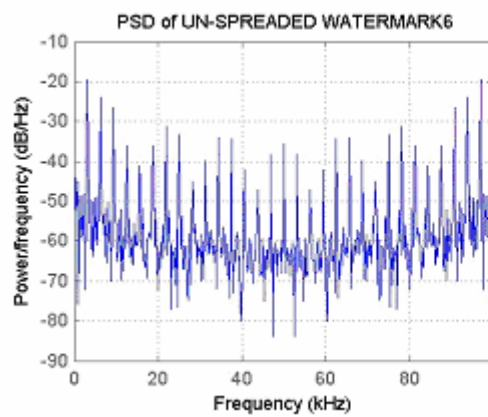
4. FRAME 4



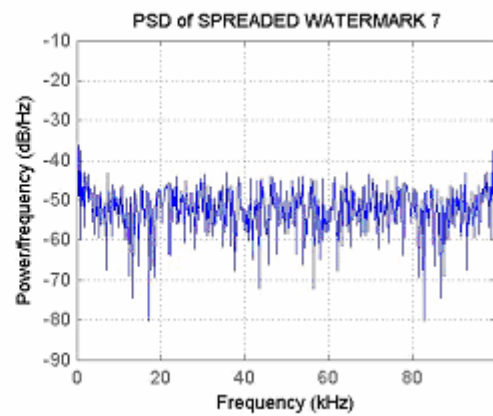
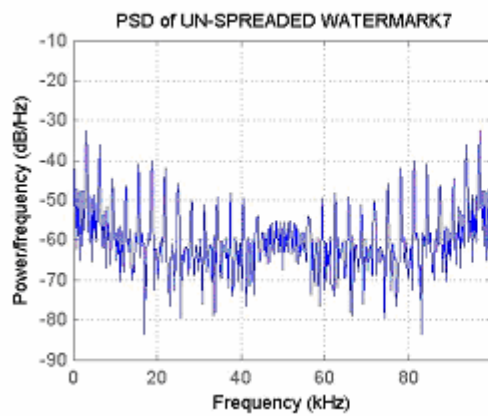
5. FRAME 5



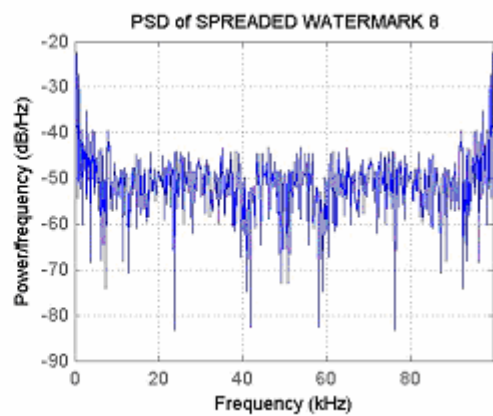
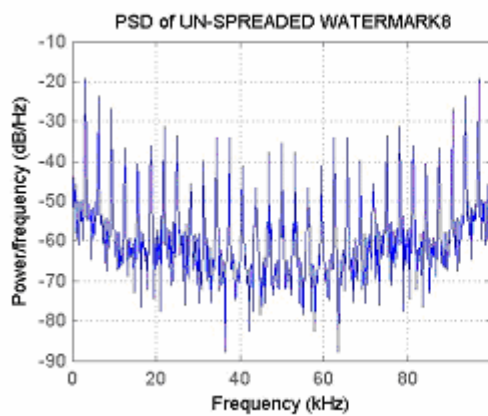
6. FRAME 6



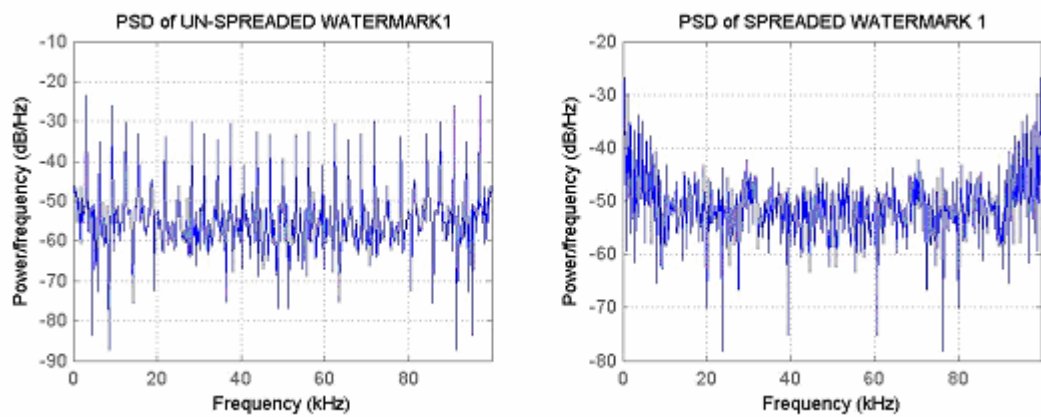
7. FRAME 7



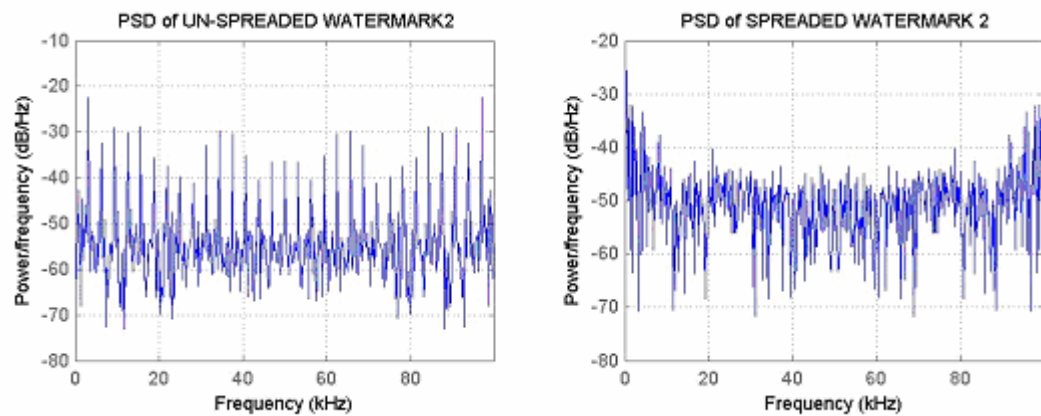
8. FRAME 8



9. FRAME 9

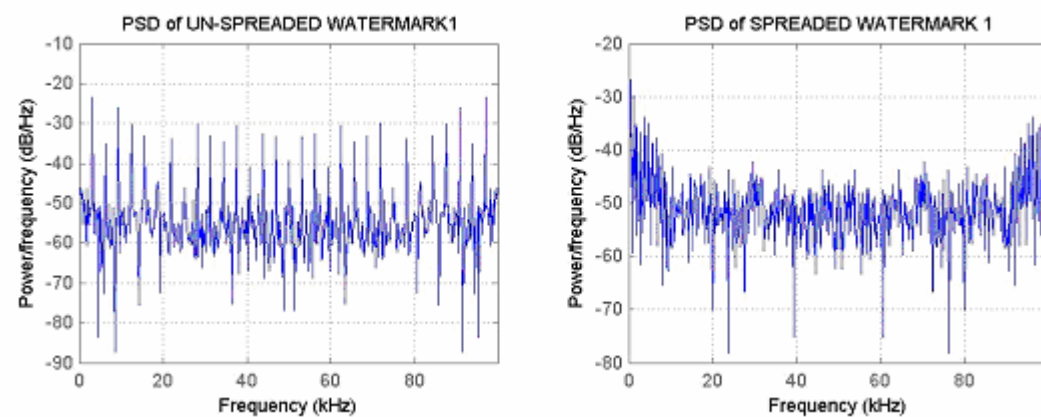


10. FRAME 10

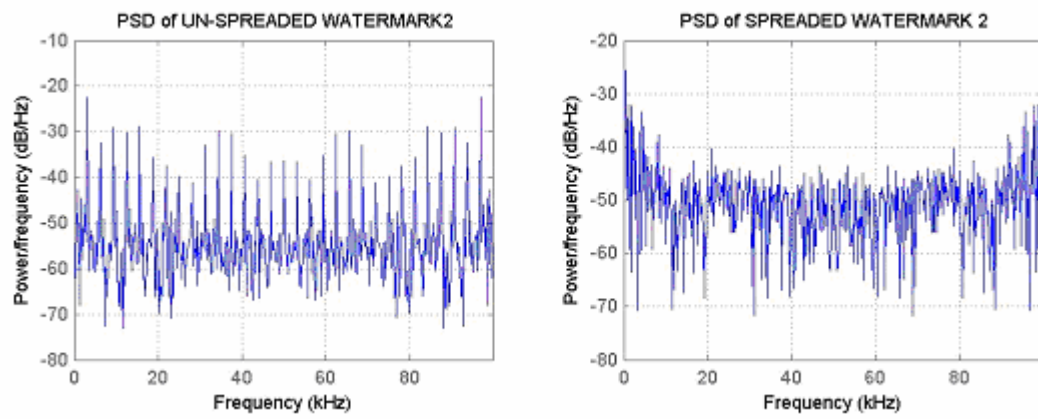


PERIDODOGRAM DISPLAY (WATERMARKING LSB PLANES)

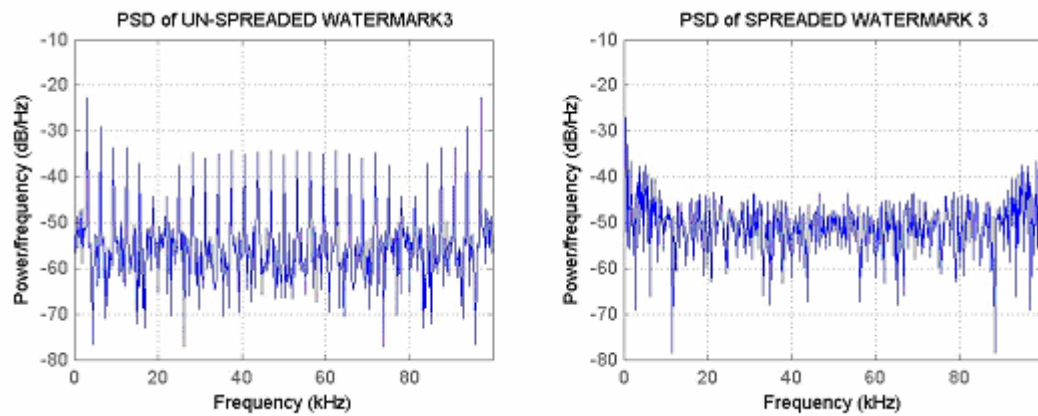
1. FRAME 1



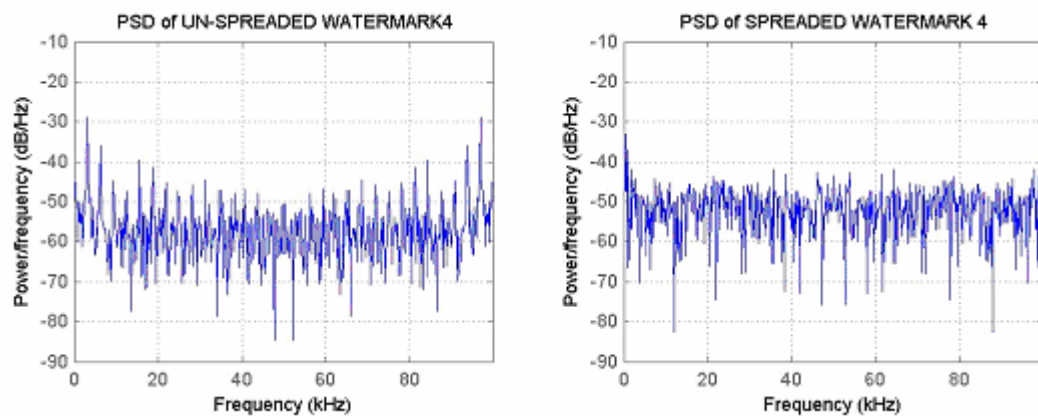
2. FRAME 2



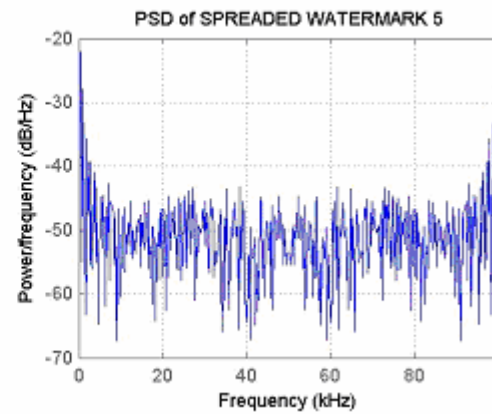
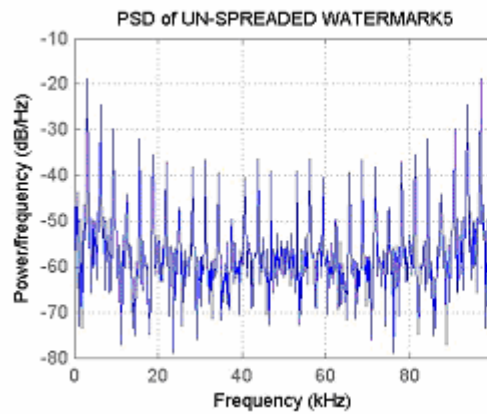
3. FRAME 3



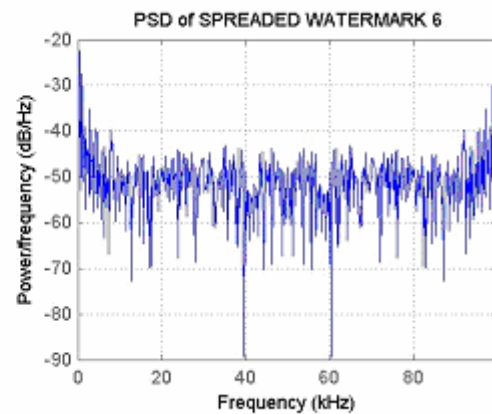
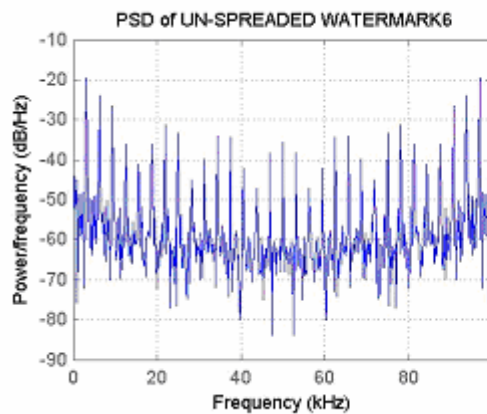
4. FRAME 4



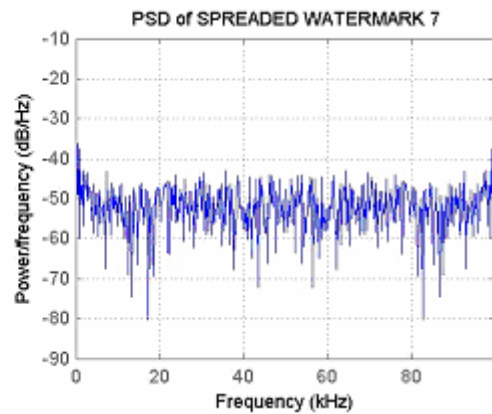
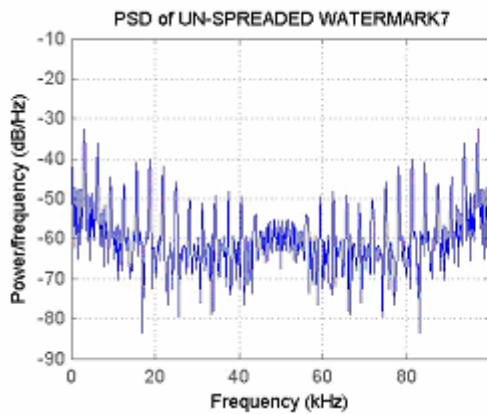
5. FRAME 5



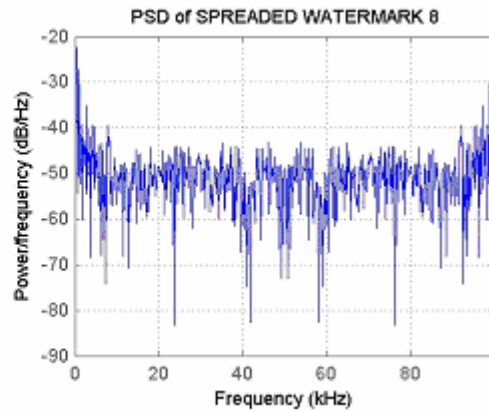
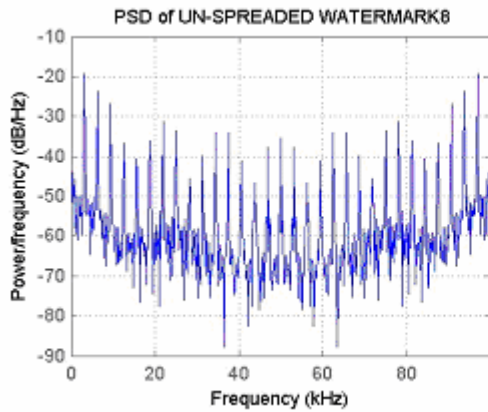
6. FRAME 6



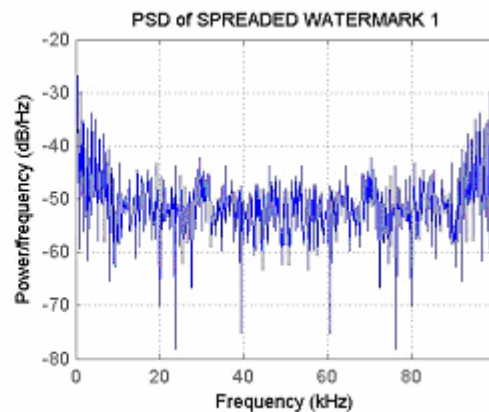
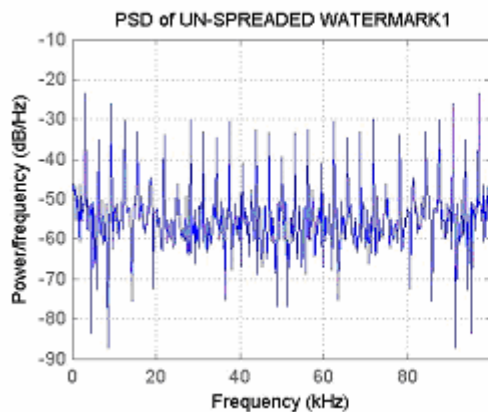
7. FRAME 7



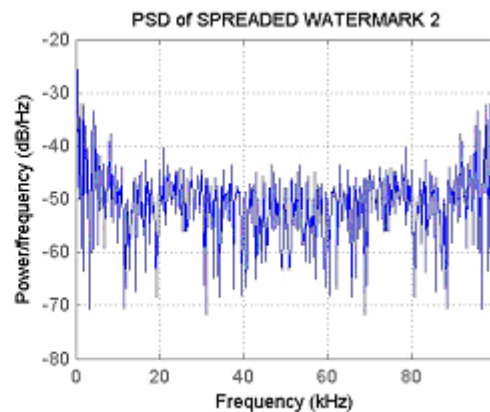
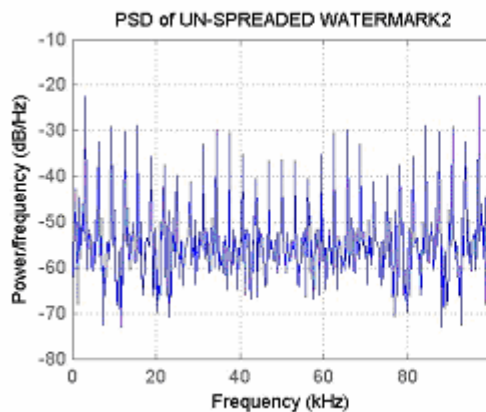
8. FRAME 8



9. FRAME 9



10. FRAME 10



SIMULATION RESULTS

SIMULATION RESULTS (WATERMARKING MSB PLANES)

WATERMARK INSERTION:

Select one of the clipped video (movie1.avi or movie2.avi): movie1.avi

MOVIE TO FRAMES SPLITTING DONE!!!!

```
*****
INTENSITY FRAMES COLLECTED!!!!
*****
FRAME TO BITPLANES SPLITTING DONE!!!!
*****
PSEUDO RANDOM SEQUENCE HAS BEEN GENERATED !!!!
*****
TAGGED AND UNTAGGED PLANES HAS BEEN SEPARATED!!!!
*****
REQUIRED NUMBER OF WATERMARKS HAVE BEEN GENERATED!!!!
*****
SPREADED WATERMARKS AND UNTAGGED BITPLANES HAVE BEEN MERGED TOGETHER!!!!
*****
INTENSITY FRAMES HAVE BEEN GENERATED!!!!
*****
COMPLETE FRAMES HAVE BEEN GENERATED!!!!
```

```
PSNR VALUE IS (IN DB) : 21.1373280 !!!!
PSNR VALUE IS (IN DB) : 10.2222053 !!!!
PSNR VALUE IS (IN DB) : 9.4441046 !!!!
PSNR VALUE IS (IN DB) : 3.8349932 !!!!
PSNR VALUE IS (IN DB) : 3.9211446 !!!!
PSNR VALUE IS (IN DB) : 15.4932113 !!!!
PSNR VALUE IS (IN DB) : 9.8494126 !!!!
PSNR VALUE IS (IN DB) : 21.1139996 !!!!
PSNR VALUE IS (IN DB) : 21.0313934 !!!!
PSNR VALUE IS (IN DB) : 9.7978324 !!!!
```

```
*****
NOW PLEASE ENTER THE WEIGHTING FACTOR
weighting factor 1(lsb) : 1
weighting factor 2 : 1
weighting factor 3 : 1
weighting factor 4 : 1
weighting factor 5 : 1
weighting factor 6 : 1
weighting factor 7 : 1
weighting factor 8(msb) : 1
*****
WPSNR VALUE IS : 11.8770499 (IN DB) !!!!
*****
TOTAL PROCESSING TIME IS : 283.6250000(IN SEC) !!!!
*****
```

filetype = .jpg

Warning: The frame height has been padded to be a multiple of four as required by the specified codec.

> In avifile.addframe at 150

In avi_joiner1 at 44

In main at 143

Warning: The frame width has been padded to be a multiple of four as required by the specified codec.

> In avifile.addframe at 156

In avi_joiner1 at 44

In main at 143

```
*****
MOVIE " MOVIE_WATERMARKED.avi " IS READY FOR DISPLAY!!!!!!!!!!
*****
```

[ATTACKING WATERMARKED VIDEO:](#)

```
*****
```

ALL THE ATTACKS ON THE WATERMARKED VIDEO HAVE BEEN PERFORMED

TOTAL ATTACKING TIME IS : 24.5000000 !!!!

WATERMARK DETECTION:

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 1

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 13.74624 (IN DB) !!!!

PSNR VALUE : 14.37322 (IN DB) !!!!

PSNR VALUE : 13.22318 (IN DB) !!!!

PSNR VALUE : 110.00000 (IN DB) !!!!

PSNR VALUE : 110.00000 (IN DB) !!!!

PSNR VALUE : 14.58184 (IN DB) !!!!

PSNR VALUE : 110.00000 (IN DB) !!!!

PSNR VALUE : 13.70178 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

weighting factor 1(lsb) : 1

weighting factor 2 : 1

weighting factor 3 : 1

weighting factor 4 : 1

weighting factor 5 : 1

weighting factor 6 : 1

weighting factor 7 : 1

weighting factor 8(msb) : 1

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 105.74031 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18881.09552 !!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18881.09552 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.76027(IN DB) !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

WATERMARKING OF DIGITAL VIDEO

WATERMARKING OF DIGITAL VIDEO

TOTAL DETECTION TIME IS : 181.8593750 !!!!

67

WATERMARKING OF DIGITAL VIDEO

[illegible]

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 4

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 13.63862 (IN DB) !!!!

PSNR VALUE : 14.24574 (IN DB) !!!!

PSNR VALUE : 12.94225 (IN DB) !!!!

PSNR VALUE : 110.00000 (IN DB) !!!!

PSNR VALUE : 110.00000 (IN DB) !!!!

PSNR VALUE : 14.28611 (IN DB) !!!!

PSNR VALUE : 110.00000 (IN DB) !!!!

PSNR VALUE : 13.52305 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

weighting factor 1(lsb) : 1

weighting factor 2 : 1

weighting factor 3 : 1

weighting factor 4 : 1

weighting factor 5 : 1

weighting factor 6 : 1

weighting factor 7 : 1

weighting factor 8(msb) : 1

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 105.74031 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18877.01789 !!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18877.01789 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.75933(IN DB) !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!

WATERMARKING OF DIGITAL VIDEO

WATERMARKING OF DIGITAL VIDEO

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 7

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 8.56319 (IN DB) !!!!

PSNR VALUE : 12.27393 (IN DB) !!!!

PSNR VALUE : 10.46367 (IN DB) !!!!

PSNR VALUE : 13.11768 (IN DB) !!!!

PSNR VALUE : 13.05630 (IN DB) !!!!

PSNR VALUE : 11.19880 (IN DB) !!!!

PSNR VALUE : 12.78880 (IN DB) !!!!

PSNR VALUE : 8.56486 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

weighting factor 1(lsb) : 1

weighting factor 2 : 1

weighting factor 3 : 1

weighting factor 4 : 1

weighting factor 5 : 1

weighting factor 6 : 1

weighting factor 7 : 1

weighting factor 8(msb) : 1

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 11.58644 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18130.88184 !!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18130.88184 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.58419(IN DB) !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

WATERMARKING OF DIGITAL VIDEO

[illegible]

weighting factor 7 : 1

WATERMARKING OF DIGITAL VIDEO

TOTAL DETECTION TIMERS : 511:7612900

|||||

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 10

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 13.79283 (IN DB) !!!!

PSNR VALUE : 14.24574 (IN DB) !!!!

PSNR VALUE : 13.11768 (IN DB) !!!!

PSNR VALUE : 110.00000 (IN DB) !!!!

PSNR VALUE : 5.39975 (IN DB) !!!!

PSNR VALUE : 4.92766 (IN DB) !!!!

PSNR VALUE : 6.19429 (IN DB) !!!!

PSNR VALUE : 7.60822 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

weighting factor 1(lsb) : 1

weighting factor 2 : 1

weighting factor 3 : 1

weighting factor 4 : 1

weighting factor 5 : 1

weighting factor 6 : 1

weighting factor 7 : 1

weighting factor 8(msb) : 1

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 100.96910 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 17006.34994 !!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 17006.34994 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.30611(IN DB) !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!

*****CORRELATING WITH RANDOM3(UNATTACKED)*****

WATERMARKING OF DIGITAL VIDEO

WATERMARKING OF DIGITAL VIDEO

PSNR VALUE : 4.92766 (IN DB) !!!!

PSNR VALUE : 6.31251 (IN DB) !!!!

PSNR VALUE : 5.44249 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

weighting factor 1(lsb) : 1

weighting factor 2 : 1

weighting factor 3 : 1

weighting factor 4 : 1

weighting factor 5 : 1

weighting factor 6 : 1

weighting factor 7 : 1

weighting factor 8(msb) : 1

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 7.83133 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 15804.45155 !!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 15804.45155 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 41.98779(IN DB) !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!

*****CORRELATING WITH RANDOM3(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!

*****CORRELATING WITH RANDOM4(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.18735(IN DB) !!!!

*****CORRELATING WITH RANDOM5(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.29579(IN DB) !!!!

```
*****CORRELATING WITH RANDOM6(UNATTACKED)*****
```

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 14046.14121 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.47557(IN DB) !!!!

TOTAL DETECTION TIME IS : 236.0781250 !!!!

[illegible]

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 13

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 13.79283 (IN DB) !!!!

PSNR VALUE : 14.24574 (IN DB) !!!!

PSNR VALUE : 5.05141 (IN DB) !!!!

PSNR VALUE : 5.77166 (IN DB) !!!!

PSNR VALUE : 110.00000 (IN DB) !!!!

PSNR VALUE : 4.92766 (IN DB) !!!!

PSNR VALUE : 6.32837 (IN DB) !!!!

PSNR VALUE : 13.68028 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

weighting factor 1(lsb) : 1

weighting factor 2 : 1

weighting factor 3 : 1

weighting factor 4 : 1

weighting factor 5 : 1

weighting factor 6 : 1

weighting factor 7 : 1

weighting factor 8(msb) : 1

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 100.96910 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18445.49601 !!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18445.49601 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.65890(IN DB) !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!

*****CORRELATING WITH RANDOM3(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

WATERMARKING OF DIGITAL VIDEO

WATERMARKING OF DIGITAL VIDEO

Select one of the clipped video (movie1.avi or movie2.avi): movie1.avi

MOVIE TO FRAMES SPLITTING DONE!!!!

INTENSITY FRAMES COLLECTED!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

PSEUDO RANDOM SEQUENCE HAS BEEN GENERATED !!!!

TAGGED AND UNTAGGED PLANES HAS BEEN SEPARATED!!!!

REQUIRED NUMBER OF WATERMARKS HAVE BEEN GENERATED!!!!

SPREADED WATERMARKS AND UNTAGGED BITPLANES HAVE BEEN MERGED TOGETHER!!!!

INTENSITY FRAMES HAVE BEEN GENERATED!!!!

COMPLETE FRAMES HAVE BEEN GENERATED!!!!

PSNR VALUE IS (IN DB) : 28.2554592 !!!!

PSNR VALUE IS (IN DB) : 14.7690995 !!!!

PSNR VALUE IS (IN DB) : 9.4797588 !!!!

PSNR VALUE IS (IN DB) : 21.0468033 !!!!

PSNR VALUE IS (IN DB) : 28.0209474 !!!!

PSNR VALUE IS (IN DB) : 15.4932113 !!!!

PSNR VALUE IS (IN DB) : 25.5239925 !!!!

PSNR VALUE IS (IN DB) : 21.1139996 !!!!

PSNR VALUE IS (IN DB) : 28.0458710 !!!!

PSNR VALUE IS (IN DB) : 25.5018309 !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

weighting factor 1(lsb) : 1

weighting factor 2 : 1

weighting factor 3 : 1

weighting factor 4 : 1

weighting factor 5 : 1

weighting factor 6 : 1

weighting factor 7 : 1

weighting factor 8(msb) : 1

WPSNR VALUE IS : 20.4629089 (IN DB) !!!!

TOTAL PROCESSING TIME IS : 287.5156250(IN SEC) !!!!

filetype = .jpg

Warning: The frame height has been padded to be a multiple of four as required by the specified

codec.

```
> In avifile.addframe at 150
  In avi_joiner1 at 44
  In main at 143
```

Warning: The frame width has been padded to be a multiple of four as required by the specified

codec.

```
> In avifile.addframe at 156
  In avi_joiner1 at 44
  In main at 143
```

MOVIE " MOVIE_WATERMARKED.avi " IS READY FOR DISPLAY!!!!!!

ATTACKING WATERMARKED VIDEO:

ALL THE ATTACKS ON THE WATERMARKED VIDEO HAVE BEEN PERFORMED

TOTAL ATTACKING TIME IS : 23.5312500 !!!!

WATERMARK DETECTION:

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 1

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 12.42062 (IN DB) !!!!

PSNR VALUE : 14.52432 (IN DB) !!!!

PSNR VALUE : 11.01098 (IN DB) !!!!

PSNR VALUE : 13.65923 (IN DB) !!!!

PSNR VALUE : 12.92067 (IN DB) !!!!

PSNR VALUE : 14.58184 (IN DB) !!!!

PSNR VALUE : 14.24574 (IN DB) !!!!

PSNR VALUE : 13.70178 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

WATERMARKING OF DIGITAL VIDEO

*****CORRELATING WITH DETECTED(UNATTACKED)*****

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

*****CORRELATING WITH RANDOM3(UNATTACKED)*****

*****CORRELATING WITH RANDOM4(UNATTACKED)*****

*****CORRELATING WITH RANDOM5(UNATTACKED)*****

*****CORRELATING WITH RANDOM6(UNATTACKED)*****

[illegible]

WATERMARKING OF DIGITAL VIDEO

*****CORRELATING WITH DETECTED(UNATTACKED)*****

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

*****CORRELATING WITH RANDOM3(UNATTACKED)*****

*****CORRELATING WITH RANDOM4(UNATTACKED)*****

*****CORRELATING WITH RANDOM5(UNATTACKED)*****

*****CORRELATING WITH RANDOM6(UNATTACKED)*****

.....

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 4

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 11.95079 (IN DB) !!!!

PSNR VALUE : 14.58184 (IN DB) !!!!

PSNR VALUE : 10.98445 (IN DB) !!!!

PSNR VALUE : 13.63862 (IN DB) !!!!

PSNR VALUE : 12.39153 (IN DB) !!!!

PSNR VALUE : 14.24574 (IN DB) !!!!

PSNR VALUE : 14.00616 (IN DB) !!!!

PSNR VALUE : 13.59862 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 13.32512 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18869.20485 (IN DB)!!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18869.20485 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.75754(IN DB) !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!

*****CORRELATING WITH RANDOM3(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!

*****CORRELATING WITH RANDOM4(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.18735(IN DB) !!!!

WATERMARKING OF DIGITAL VIDEO

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!

*****CORRELATING WITH RANDOM3(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!

```
*****CORRELATING WITH RANDOM4(UNATTACKED)*****
```

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.18735(IN DB) !!!!

```
*****CORRELATING WITH RANDOM5(UNATTACKED)*****
```

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.29579(IN DB) !!!!

*****CORRELATING WITH RANDOM6(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 14046.14121 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.47557(IN DB) !!!!

TOTAL DETECTION TIME IS : 305.3906250 !!!!

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 6

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 6.94392 (IN DB) !!!!

PSNR VALUE : 8.25981 (IN DB) !!!!

PSNR VALUE : 7.33961 (IN DB) !!!!

PSNR VALUE : 8.34383 (IN DB) !!!!

PSNR VALUE : 6.78436 (IN DB) !!!!

PSNR VALUE : 8.29041 (IN DB) !!!!

PSNR VALUE : 8.19738 (IN DB) !!!!

PSNR VALUE : 7.75060 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 7.77884 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 17251.02096 (IN DB)!!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING CORRELATION VALUES!!!

WATERMARKING OF DIGITAL VIDEO

*****CORRELATING WITH DETECTED(UNATTACKED)*****

*****CORRELATING WITH ORIGINAL (UNATTACKED)*****

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

*****CORRELATING WITH RANDOM3(UNATTACKED)*****

*****CORRELATING WITH RANDOM4(UNATTACKED)*****

*****CORRELATING WITH RANDOM5(UNATTACKED)*****

*****CORRELATING WITH RANDOM6(UNATTACKED)*****

[illegible]

94

```

*****
PSNR VALUE : 11.01766 (IN DB) !!!!
*****
PSNR VALUE : 13.59862 (IN DB) !!!!
*****
PSNR VALUE : 12.87860 (IN DB) !!!!
*****
PSNR VALUE : 14.42050 (IN DB) !!!!
*****
PSNR VALUE : 14.10097 (IN DB) !!!!
*****
PSNR VALUE : 13.61842 (IN DB) !!!!
*****
NOW PLEASE ENTER THE WEIGHTING FACTOR
*****
WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 13.42684 (IN DB) !!!!
*****
CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18871.30244 (IN DB)!!!!
*****
COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****
CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18871.30244 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.75802(IN DB) !!!!
*****CORRELATING WITH ORIGINAL(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!
*****CORRELATING WITH RANDOM2(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!
*****CORRELATING WITH RANDOM3(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!
*****CORRELATING WITH RANDOM4(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.18735(IN DB) !!!!
*****CORRELATING WITH RANDOM5(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.29579(IN DB) !!!!
*****CORRELATING WITH RANDOM6(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 14046.14121 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.47557(IN DB) !!!!
*****
TOTAL DETECTION TIME IS : 313.5781250 !!!!

```

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 9

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 12.19615 (IN DB) !!!!

PSNR VALUE : 14.17033 (IN DB) !!!!

PSNR VALUE : 10.95496 (IN DB) !!!!

PSNR VALUE : 13.37065 (IN DB) !!!!

PSNR VALUE : 12.82793 (IN DB) !!!!

PSNR VALUE : 13.97665 (IN DB) !!!!

PSNR VALUE : 13.68028 (IN DB) !!!!

PSNR VALUE : 13.52305 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 13.19362 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18862.21085 (IN DB)!!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18862.21085 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.75593(IN DB) !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!

*****CORRELATING WITH RANDOM3(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!

*****CORRELATING WITH RANDOM4(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.18735(IN DB) !!!!

*****CORRELATING WITH RANDOM5(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.29579(IN DB) !!!!

*****CORRELATING WITH RANDOM6(UNATTACKED)*****

WATERMARKING OF DIGITAL VIDEO

[illegible]

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!

*****CORRELATING WITH RANDOM4(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.18735(IN DB) !!!!

*****CORRELATING WITH RANDOM5(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.29579(IN DB) !!!!

*****CORRELATING WITH RANDOM6(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 14046.14121 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.47557(IN DB) !!!!

TOTAL DETECTION TIME IS : 294.6562500 !!!!

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 11

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 5.09794 (IN DB) !!!!

PSNR VALUE : 5.42629 (IN DB) !!!!

PSNR VALUE : 4.78457 (IN DB) !!!!

PSNR VALUE : 4.91857 (IN DB) !!!!

PSNR VALUE : 5.41892 (IN DB) !!!!

PSNR VALUE : 5.52921 (IN DB) !!!!

PSNR VALUE : 4.97154 (IN DB) !!!!

PSNR VALUE : 5.50573 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 5.21541 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 14056.76959 (IN DB)!!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 14056.76959 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 41.47886(IN DB) !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

WATERMARKING OF DIGITAL VIDEO

WATERMARKING OF DIGITAL VIDEO

```

*****
PSNR VALUE : 6.13803 (IN DB) !!!!
*****
PSNR VALUE : 13.68028 (IN DB) !!!!
*****
NOW PLEASE ENTER THE WEIGHTING FACTOR
*****
WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 11.08909 (IN DB) !!!!
*****
CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18427.01009 (IN DB)!!!!
*****

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****
CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18427.01009 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.65455(IN DB) !!!!
*****CORRELATING WITH ORIGINAL(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!
*****CORRELATING WITH RANDOM2(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!
*****CORRELATING WITH RANDOM3(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!
*****CORRELATING WITH RANDOM4(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.18735(IN DB) !!!!
*****CORRELATING WITH RANDOM5(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.29579(IN DB) !!!!
*****CORRELATING WITH RANDOM6(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 14046.14121 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.47557(IN DB) !!!!
*****
TOTAL DETECTION TIME IS : 314.6718750 !!!!
*****

```

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 14

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 12.26730 (IN DB) !!!!

```

*****
PSNR VALUE : 14.47072 (IN DB) !!!!
*****
PSNR VALUE : 11.01766 (IN DB) !!!!
*****
PSNR VALUE : 5.67259 (IN DB) !!!!
*****
PSNR VALUE : 12.88899 (IN DB) !!!!
*****
PSNR VALUE : 14.42050 (IN DB) !!!!
*****
PSNR VALUE : 5.09344 (IN DB) !!!!
*****
PSNR VALUE : 13.68028 (IN DB) !!!!
*****
NOW PLEASE ENTER THE WEIGHTING FACTOR
*****
WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 12.26828 (IN DB) !!!!
*****
CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18496.76333 (IN DB)!!!!
*****
COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****
CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18496.76333 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.67096(IN DB) !!!!
*****CORRELATING WITH ORIGINAL(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!
*****CORRELATING WITH RANDOM2(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!
*****CORRELATING WITH RANDOM3(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!
*****CORRELATING WITH RANDOM4(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.18735(IN DB) !!!!
*****CORRELATING WITH RANDOM5(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.29579(IN DB) !!!!
*****CORRELATING WITH RANDOM6(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 14046.14121 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.47557(IN DB) !!!!
*****
TOTAL DETECTION TIME IS : 191.1250000 !!!!

```

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 15

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 8.99353 (IN DB) !!!!

PSNR VALUE : 9.58391 (IN DB) !!!!

PSNR VALUE : 8.93793 (IN DB) !!!!

PSNR VALUE : 9.89840 (IN DB) !!!!

PSNR VALUE : 9.14354 (IN DB) !!!!

PSNR VALUE : 9.53494 (IN DB) !!!!

PSNR VALUE : 9.90959 (IN DB) !!!!

PSNR VALUE : 9.45658 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 9.44666 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 17806.12317 (IN DB)!!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 17806.12317 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.50569(IN DB) !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!

*****CORRELATING WITH RANDOM3(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!

*****CORRELATING WITH RANDOM4(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.18735(IN DB) !!!!

*****CORRELATING WITH RANDOM5(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.29579(IN DB) !!!!

*****CORRELATING WITH RANDOM6(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 14046.14121 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.47557(IN DB) !!!!

TOTAL DETECTION TIME IS : 307.3125000 !!!!

SIMULATION RESULTS (WATERMARKING LSB PLANES)

WATERMARK INSERTION :

Select one of the clipped video (movie1.avi or movie2.avi): movie1.avi

MOVIE TO FRAMES SPLITTING DONE!!!!

INTENSITY FRAMES COLLECTED!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

PSEUDO RANDOM SEQUENCE HAS BEEN GENERATED !!!!

TAGGED AND UNTAGGED PLANES HAS BEEN SEPARATED!!!!

REQUIRED NUMBER OF WATERMARKS HAVE BEEN GENERATED!!!!

SPREADED WATERMARKS AND UNTAGGED BITPLANES HAVE BEEN MERGED TOGETHER!!!!

INTENSITY FRAMES HAVE BEEN GENERATED!!!!

COMPLETE FRAMES HAVE BEEN GENERATED!!!!

PSNR VALUE IS (IN DB) : 29.4989095 !!!!

PSNR VALUE IS (IN DB) : 20.6556147 !!!!

PSNR VALUE IS (IN DB) : 9.4727591 !!!!

PSNR VALUE IS (IN DB) : 28.1443822 !!!!

PSNR VALUE IS (IN DB) : 29.2770276 !!!!

PSNR VALUE IS (IN DB) : 29.1895326 !!!!

PSNR VALUE IS (IN DB) : 28.8403140 !!!!

PSNR VALUE IS (IN DB) : 29.0643223 !!!!

PSNR VALUE IS (IN DB) : 29.2715480 !!!!

PSNR VALUE IS (IN DB) : 25.5018309 !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

weighting factor 1(lsb) : 1


```
weighting factor 2 : 1
weighting factor 3 : 1
weighting factor 4 : 1
weighting factor 5 : 1
weighting factor 6 : 1
weighting factor 7 : 1
weighting factor 8(msb) : 1
*****
```

WPSNR VALUE IS : 25.5178578 (IN DB) !!!!

TOTAL PROCESSING TIME IS : 285.4531250(IN SEC) !!!!

```
filetype = .jpg
```

Warning: The frame height has been padded to be a multiple of four as required by the specified codec.

> In avifile.addframe at 150

In avi_joiner1 at 44

In main at 143

Warning: The frame width has been padded to be a multiple of four as required by the specified codec.

```
> In avifile.addframe at 156
```

In avi_joiner1 at 44

In main at 143

MOVIE " MOVIE_WATERMARKED.avi " IS READY FOR DISPLAY!!!!!!!!!!

[illegible]

ATTACKING WATERMARKED VIDEO:

ALL THE ATTACKS ON THE WATERMARKED VIDEO HAVE BEEN PERFORMED

TOTAL ATTACKING TIME IS : 23.5312500 !!!!

[illegible]

WATERMARK DETECTION:

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 1

MOVIE TO FRAMES SPLITTING DONE!!!!

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 2

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 5.46899 (IN DB) !!!!

PSNR VALUE : 6.25342 (IN DB) !!!!

PSNR VALUE : 5.86898 (IN DB) !!!!

PSNR VALUE : 6.36872 (IN DB) !!!!

PSNR VALUE : 5.16378 (IN DB) !!!!

PSNR VALUE : 5.35248 (IN DB) !!!!

PSNR VALUE : 6.24476 (IN DB) !!!!

PSNR VALUE : 5.44397 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 5.79322 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 15749.19460 (IN DB)!!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 15749.19460 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 41.97258(IN DB) !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!

*****CORRELATING WITH RANDOM3(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!

*****CORRELATING WITH RANDOM4(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

WATERMARKING OF DIGITAL VIDEO

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 14046.14121 !!!!

TOTAL DETECTION TIME IS : 179.4843750 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

WATERMARKING OF DIGITAL VIDEO

WATERMARKING OF DIGITAL VIDEO

[illegible]

111


```

*****
PSNR VALUE : 7.67921 (IN DB) !!!!
*****
PSNR VALUE : 6.38745 (IN DB) !!!!
*****
PSNR VALUE : 7.48675 (IN DB) !!!!
*****
PSNR VALUE : 5.18765 (IN DB) !!!!
*****
PSNR VALUE : 6.04271 (IN DB) !!!!
*****
PSNR VALUE : 6.93520 (IN DB) !!!!
*****
PSNR VALUE : 6.02825 (IN DB) !!!!
*****
NOW PLEASE ENTER THE WEIGHTING FACTOR
*****
WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 6.49070 (IN DB) !!!!
*****
CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 16225.43409 (IN DB)!!!!
*****

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****
CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 16225.43409 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.10196(IN DB) !!!!
*****CORRELATING WITH ORIGINAL(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!
*****CORRELATING WITH RANDOM2(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!
*****CORRELATING WITH RANDOM3(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!
*****CORRELATING WITH RANDOM4(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.18735(IN DB) !!!!
*****CORRELATING WITH RANDOM5(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.29579(IN DB) !!!!
*****CORRELATING WITH RANDOM6(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 14046.14121 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.47557(IN DB) !!!!
*****
TOTAL DETECTION TIME IS : 313.5781250 !!!!

```

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 7

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 5.61124 (IN DB) !!!!

PSNR VALUE : 6.95701 (IN DB) !!!!

PSNR VALUE : 5.97329 (IN DB) !!!!

PSNR VALUE : 6.57198 (IN DB) !!!!

PSNR VALUE : 5.17721 (IN DB) !!!!

PSNR VALUE : 5.50866 (IN DB) !!!!

PSNR VALUE : 6.37016 (IN DB) !!!!

PSNR VALUE : 5.46163 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 5.99368 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 15757.47738 (IN DB)!!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 15757.47738 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 41.97487(IN DB) !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!

*****CORRELATING WITH RANDOM3(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!

*****CORRELATING WITH RANDOM4(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.18735(IN DB) !!!!

*****CORRELATING WITH RANDOM5(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.29579(IN DB) !!!!

*****CORRELATING WITH RANDOM6(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 14046.14121 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.47557(IN DB) !!!!

TOTAL DETECTION TIME IS : 305.0468750 !!!!

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 8

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 5.50866 (IN DB) !!!!

PSNR VALUE : 13.46977 (IN DB) !!!!

PSNR VALUE : 9.62934 (IN DB) !!!!

PSNR VALUE : 12.55948 (IN DB) !!!!

PSNR VALUE : 5.23681 (IN DB) !!!!

PSNR VALUE : 9.62104 (IN DB) !!!!

PSNR VALUE : 10.22944 (IN DB) !!!!

PSNR VALUE : 9.83199 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 10.29709 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18191.87813 (IN DB)!!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18191.87813 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.59878(IN DB) !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!

*****CORRELATING WITH RANDOM3(UNATTACKED)*****

WATERMARKING OF DIGITAL VIDEO

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.59620(IN DB) !!!!
 *****CORRELATING WITH ORIGINAL(UNATTACKED)*****
 CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!
 *****CORRELATING WITH RANDOM2(UNATTACKED)*****
 CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!
 *****CORRELATING WITH RANDOM3(UNATTACKED)*****
 CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!
 *****CORRELATING WITH RANDOM4(UNATTACKED)*****
 CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.18735(IN DB) !!!
 *****CORRELATING WITH RANDOM5(UNATTACKED)*****
 CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.29579(IN DB) !!!
 *****CORRELATING WITH RANDOM6(UNATTACKED)*****
 CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 14046.14121 !!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.47557(IN DB) !!!!

 TOTAL DETECTION TIME IS : 307.2031250 !!!!

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 10

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 54.0985 (IN DB) !!!!

PSNR VALUE : 13.46977 (IN DB) !!!!

PSNR VALUE : 9.64391 (IN DB) !!!!

PSNR VALUE : 12.55139 (IN DB) !!!!

 DSNB VALUE = 5.14286 (IN DB) !!!

 DSNB VALUE = 651860 (IN DB) !!!

 DSNB VALUE = 6.89001 (IN DB) III

```
*****
PSNR VALUE : 4.95794 (IN DB) !!!!
*****
PSNR VALUE : 5.39237 (IN DB) !!!!
*****
PSNR VALUE : 5.46751 (IN DB) !!!!
*****
PSNR VALUE : 4.94735 (IN DB) !!!!
*****
PSNR VALUE : 5.48222 (IN DB) !!!!
*****
NOW PLEASE ENTER THE WEIGHTING FACTOR
*****
WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 5.20732 (IN DB) !!!!
*****
CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 14080.20851 (IN DB)!!!!
*****

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****
CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 14080.20851 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 41.48609(IN DB) !!!!
*****CORRELATING WITH ORIGINAL(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!
*****CORRELATING WITH RANDOM2(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!
*****CORRELATING WITH RANDOM3(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!
*****CORRELATING WITH RANDOM4(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.18735(IN DB) !!!!
*****CORRELATING WITH RANDOM5(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.29579(IN DB) !!!!
*****CORRELATING WITH RANDOM6(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 14046.14121 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.47557(IN DB) !!!!
*****
TOTAL DETECTION TIME IS : 305.8750000 !!!!
*****
```

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked) : 12

```
*****
```

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 5.49985 (IN DB) !!!!

PSNR VALUE : 5.68135 (IN DB) !!!!

PSNR VALUE : 6.09616 (IN DB) !!!!

PSNR VALUE : 5.74983 (IN DB) !!!!

PSNR VALUE : 5.14286 (IN DB) !!!!

PSNR VALUE : 6.51862 (IN DB) !!!!

PSNR VALUE : 6.75686 (IN DB) !!!!

PSNR VALUE : 5.31696 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 5.87860 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 16067.53853 (IN DB)!!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 16067.53853 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.05949(IN DB) !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!

*****CORRELATING WITH RANDOM3(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!

*****CORRELATING WITH RANDOM4(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.18735(IN DB) !!!!

*****CORRELATING WITH RANDOM5(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.29579(IN DB) !!!!

*****CORRELATING WITH RANDOM6(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 14046.14121 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.47557(IN DB) !!!!

TOTAL DETECTION TIME IS : 296.2031250 !!!!

Enter the number corresponding to the Watermarked Video (Attacked or Un-attacked): 13

MOVIE TO FRAMES SPLITTING DONE!!!!

FRAME TO BITPLANES SPLITTING DONE!!!!

WATERMARK HAS BEEN DE-SPREADED!!!!

PSNR VALUE : 5.49985 (IN DB) !!!!

PSNR VALUE : 13.46977 (IN DB) !!!!

PSNR VALUE : 6.09616 (IN DB) !!!!

PSNR VALUE : 5.85737 (IN DB) !!!!

PSNR VALUE : 5.22044 (IN DB) !!!!

PSNR VALUE : 6.51862 (IN DB) !!!!

PSNR VALUE : 7.37665 (IN DB) !!!!

PSNR VALUE : 9.82760 (IN DB) !!!!

NOW PLEASE ENTER THE WEIGHTING FACTOR

WPSNR VALUE IN CASE OF DETECTED WATERMARK IS : 8.49667 (IN DB) !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18222.17953 (IN DB)!!!!

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING
CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 18222.17953 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.60600(IN DB) !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!

*****CORRELATING WITH RANDOM2(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!

*****CORRELATING WITH RANDOM3(UNATTACKED)*****

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

WATERMARKING OF DIGITAL VIDEO

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 14046.14121 !!!!

TOTAL DETECTION TIME IS : 302.2187500 !!!!

*****CORRELATING WITH ORIGINAL(UNATTACKED)*****

WATERMARKING OF DIGITAL VIDEO

COMPARING DETECTED & OTHER RANDOMLY GENERATED WATERMARKS USING CORRELATION VALUES!!!

*****CORRELATING WITH DETECTED(UNATTACKED)*****
CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 17250.30693 !!!!

CORRELATION VALUE IN CASE OF DETECTED WATERMARK IS : 42.36797(IN DB) !!!!
 *****CORRELATING WITH ORIGINAL(UNATTACKED)*****
 CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 18896.55737 !!!!

```

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 42.76383(IN DB) !!!!
*****CORRELATING WITH RANDOM2(UNATTACKED)*****
CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 12992.09412 !!!!

```

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.13679(IN DB) !!!!
 *****CORRELATING WITH RANDOM3(UNATTACKED)*****
 CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 15316.77950 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.85167(IN DB) !!!!
 *****CORRELATING WITH RANDOM4(UNATTACKED)*****
 CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13144.21272 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.18735(IN DB) !!!!
 *****CORRELATING WITH RANDOM5(UNATTACKED)*****
 CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 13476.56766 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.29579(IN DB) !!!!
 *****CORRELATING WITH RANDOM6(UNATTACKED)*****
 CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 14046.14121 !!!!

CORRELATION VALUE IN CASE OF RANDOM WATERMARK IS : 41.47557(IN DB) !!!!

 TOTAL DETECTION TIME IS : 279.9687500 !!!!

STAGE 2: ATTACKS ON WATERMARKED DIGITAL VIDEO**MODEL OF THE STAGE**

VIDEO WATERMARKING : ATTACKING WATERMARKED VIDEO

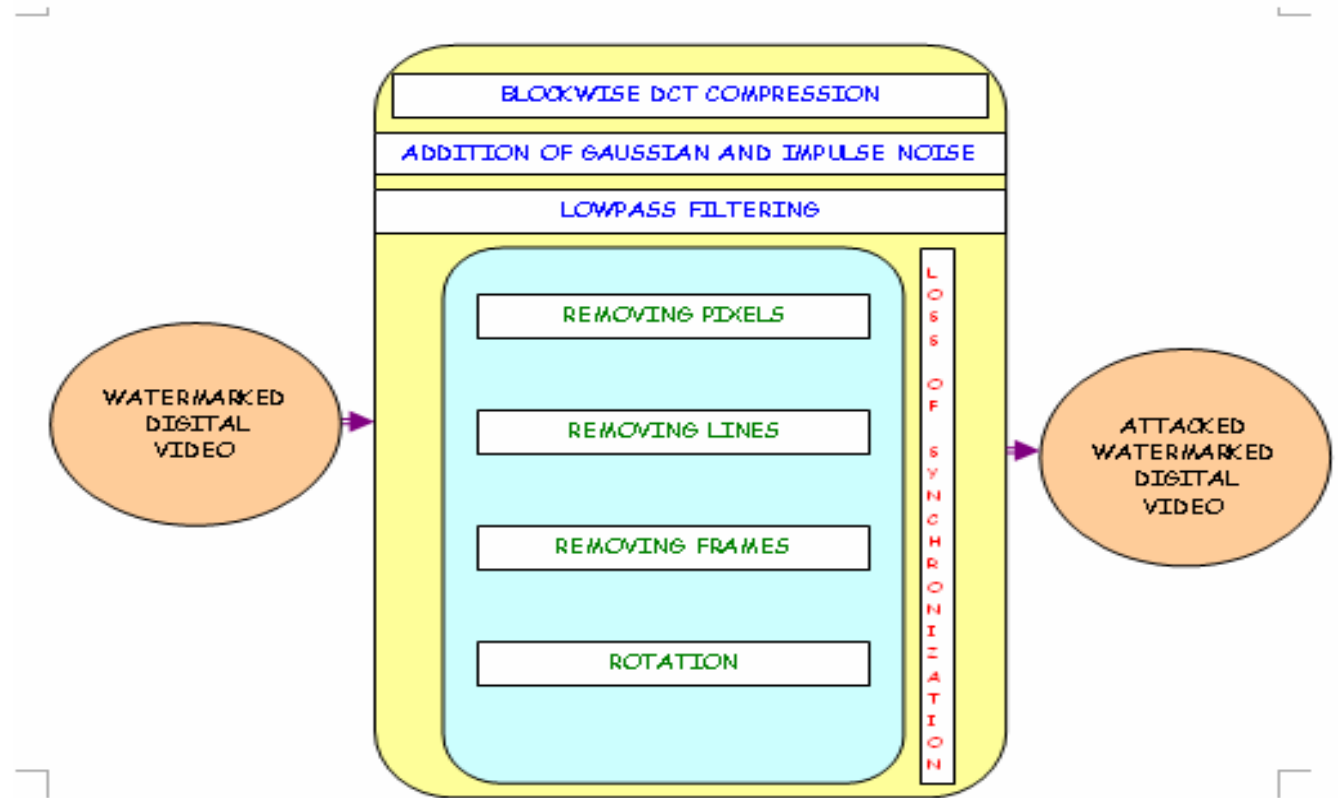
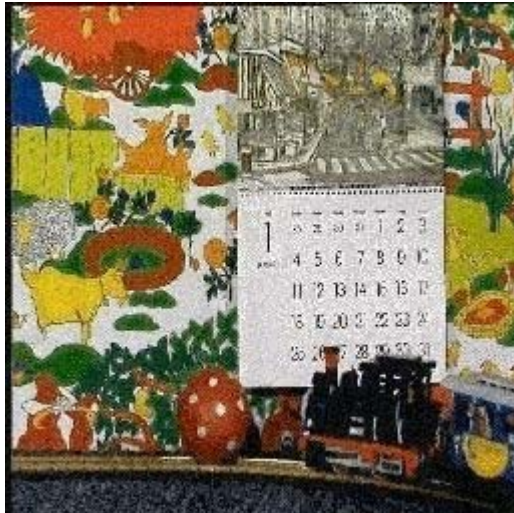
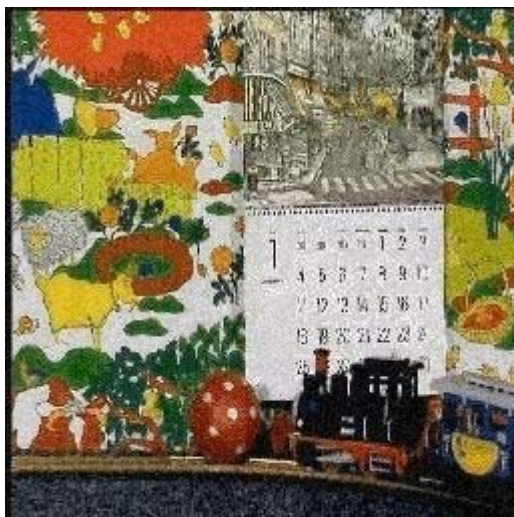
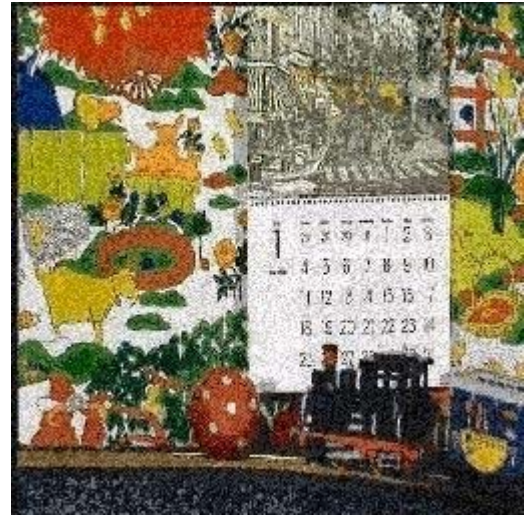


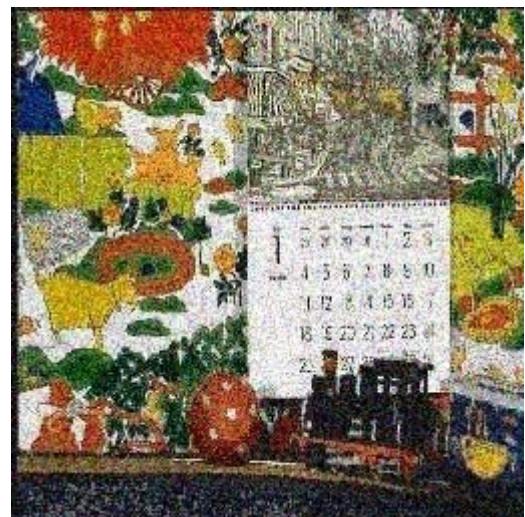
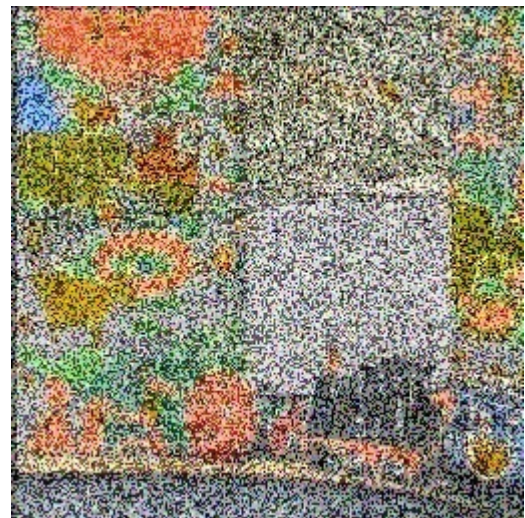
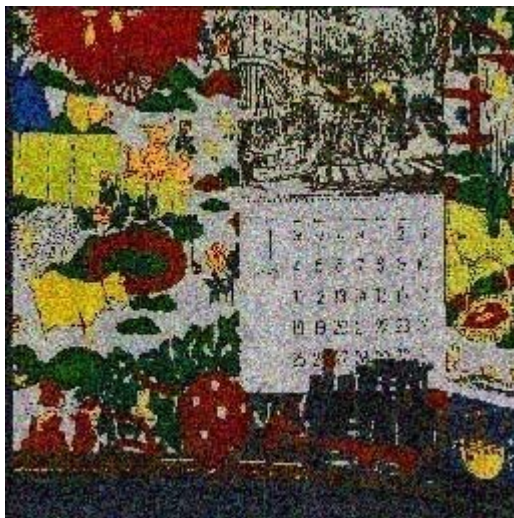
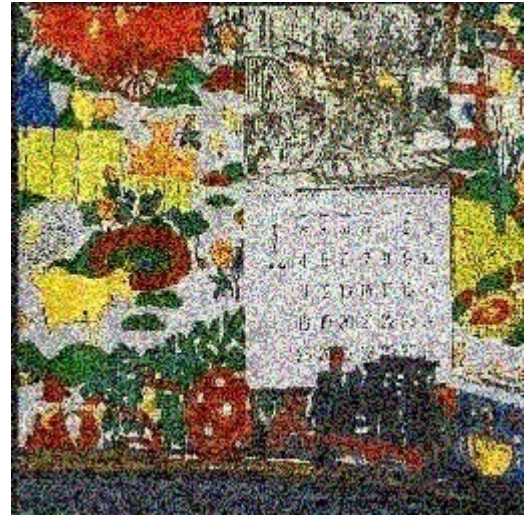
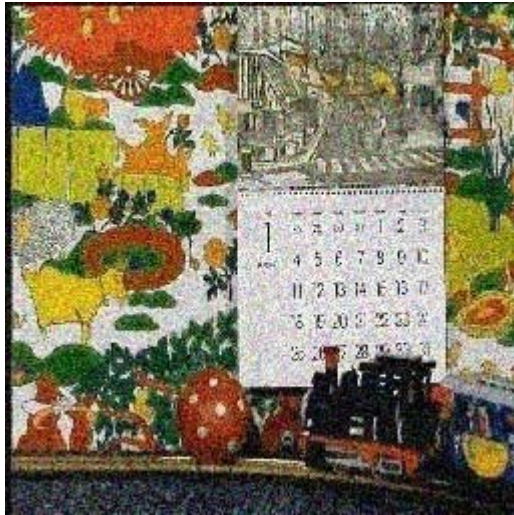
Figure 5.6 Model of the Stage II (Attacking Stage)

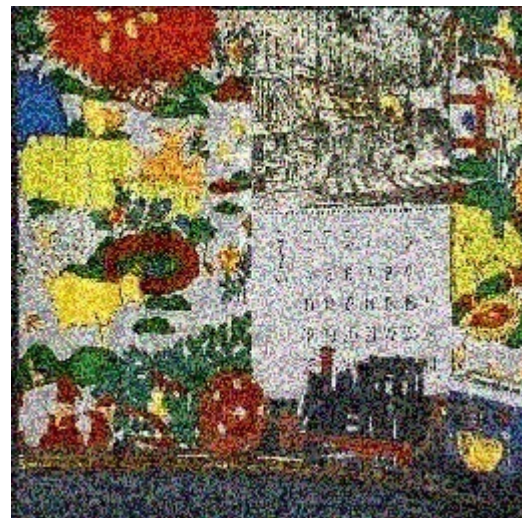
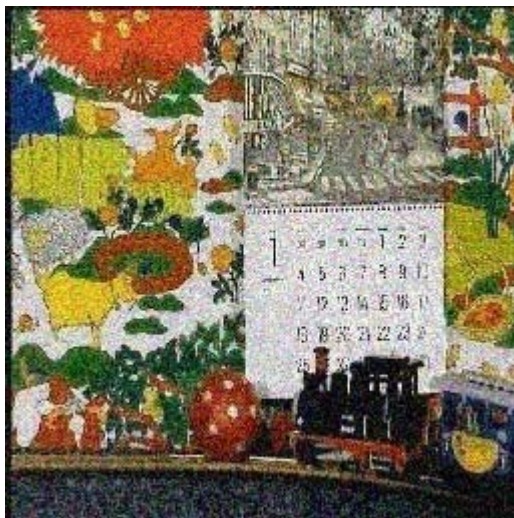
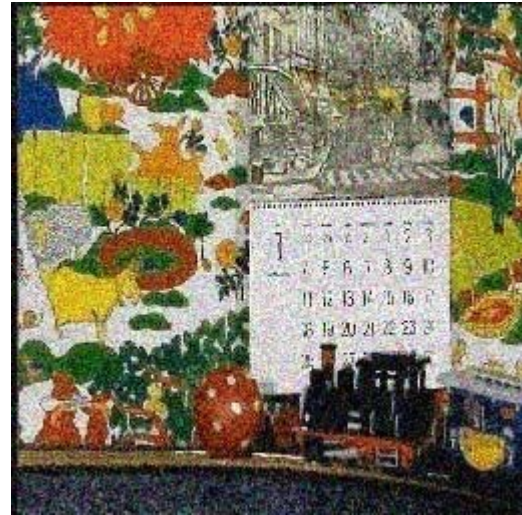
MATLAB CODE SIMULATION RESULTS

ATTACKED FRAMES
(WATERMARKING MSB PLANES)1. `compressed_video`

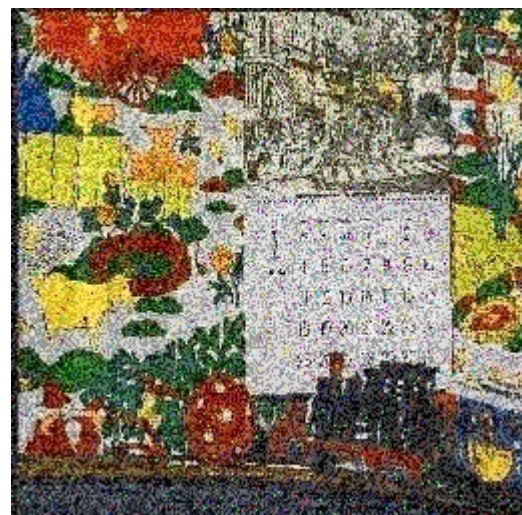
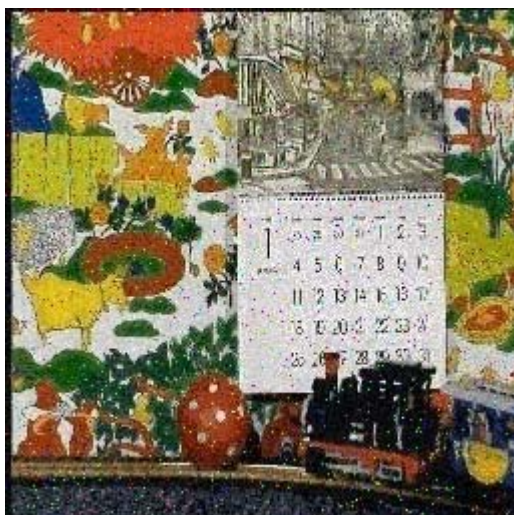


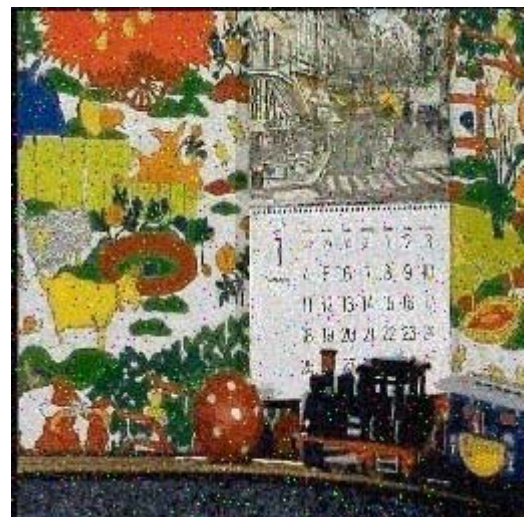
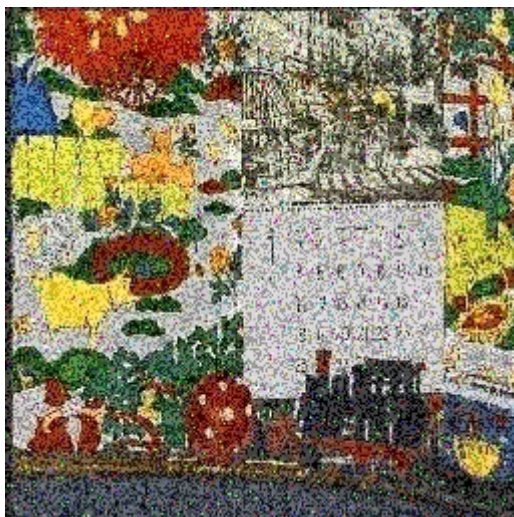
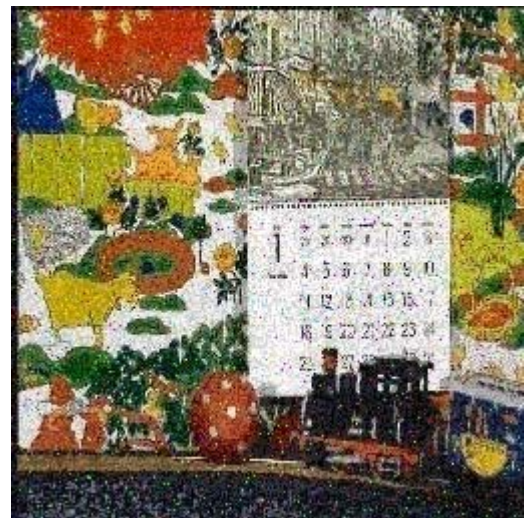
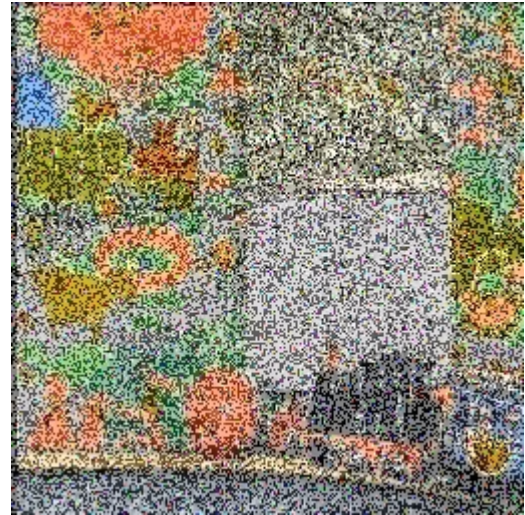
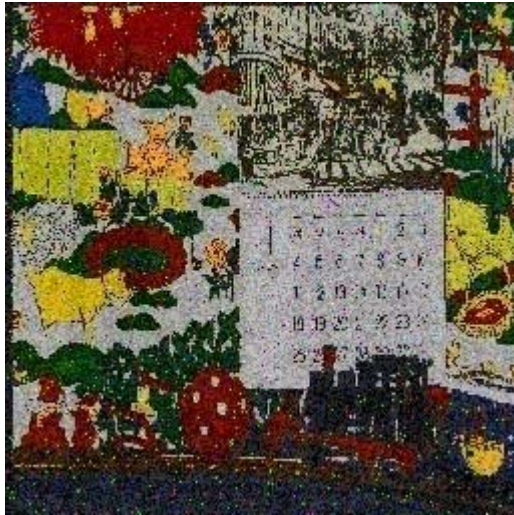
2. noisy_gaussian_video





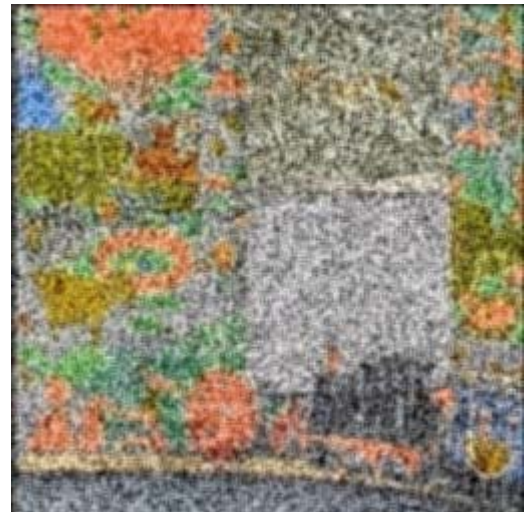
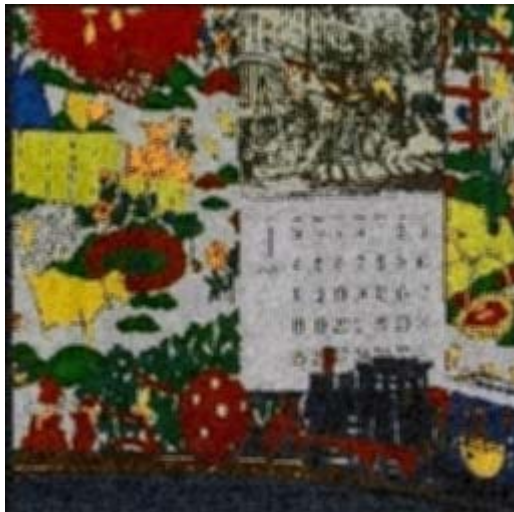
3. noisy_salt_pepper_video





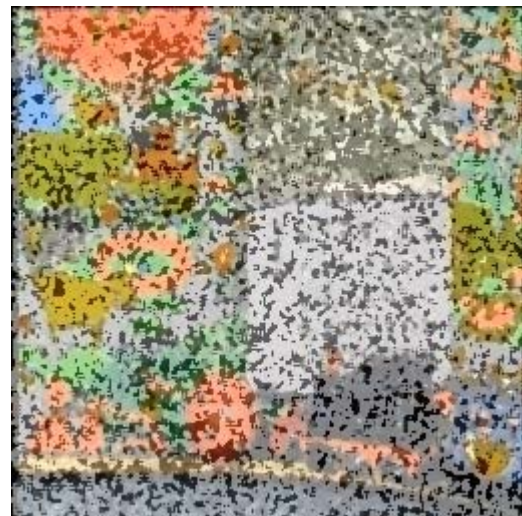


4. averaged_filtered_video



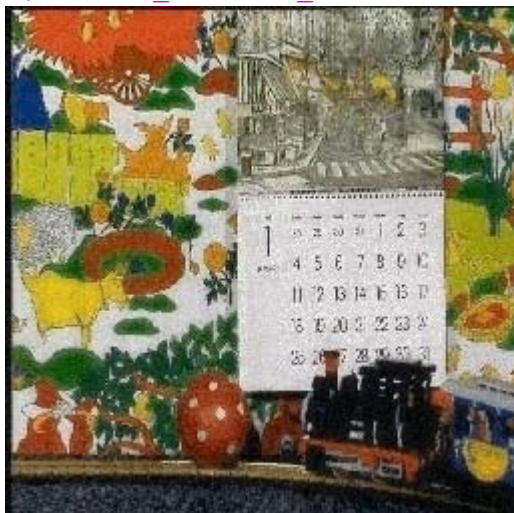


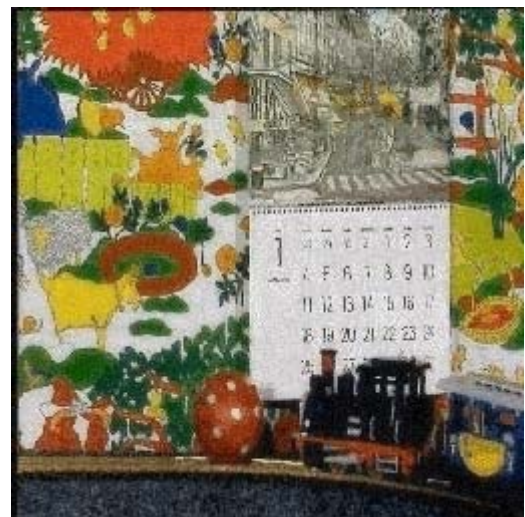
5. median_filtered_video





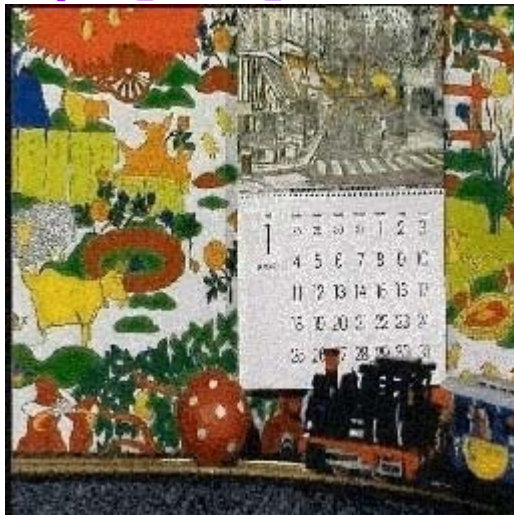
6. wiener_filtered_video

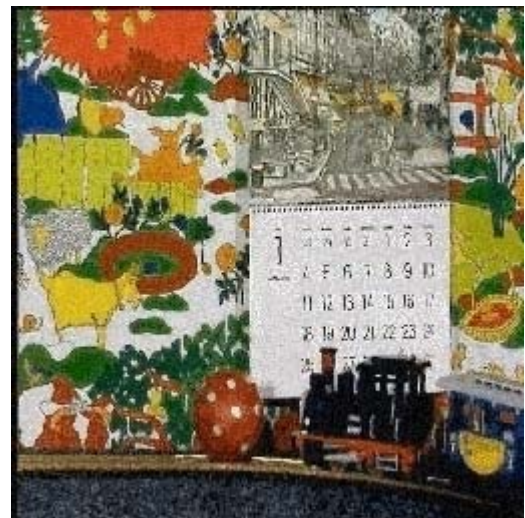




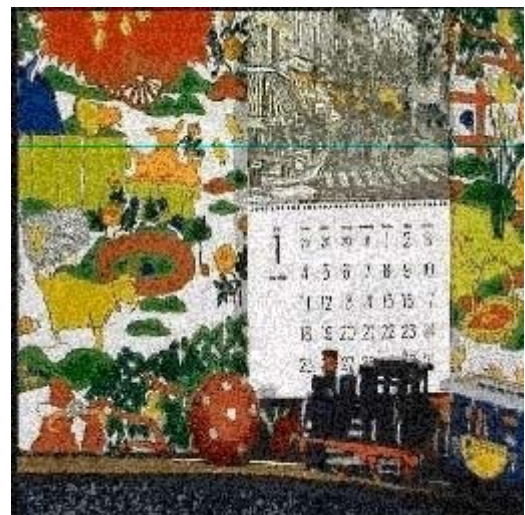
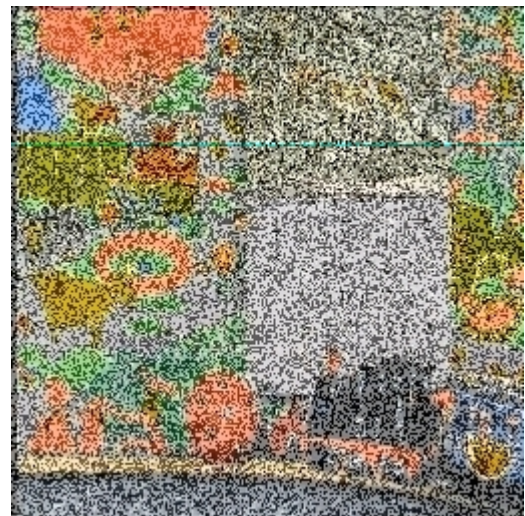
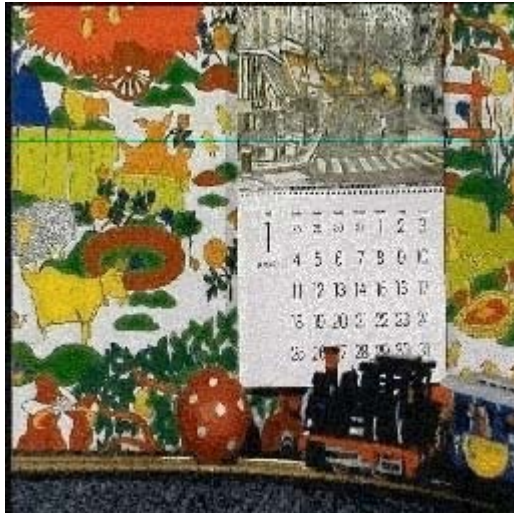


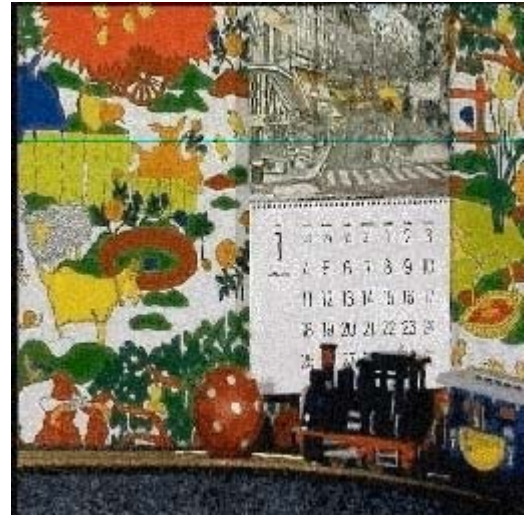
7. pixel_removed_video



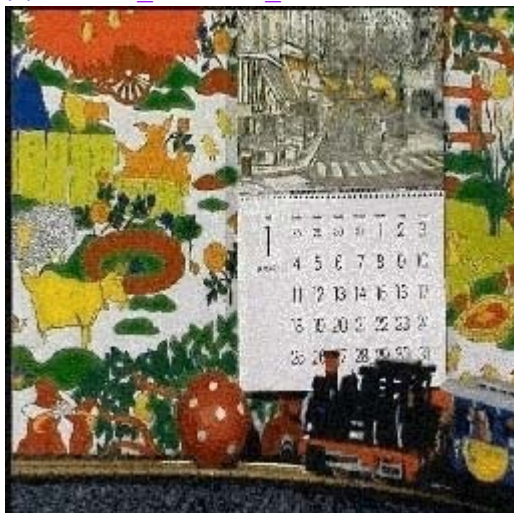


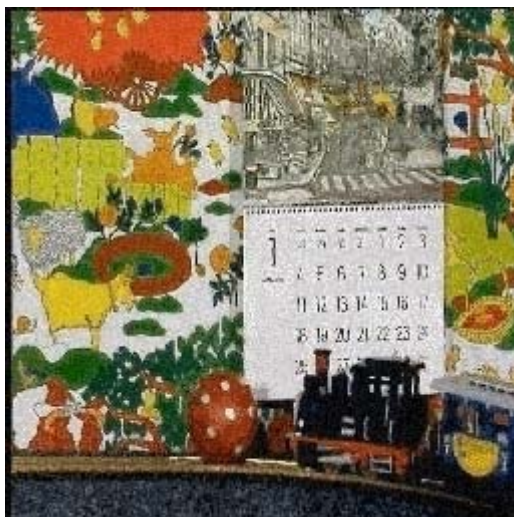
8. `line_removed_video`



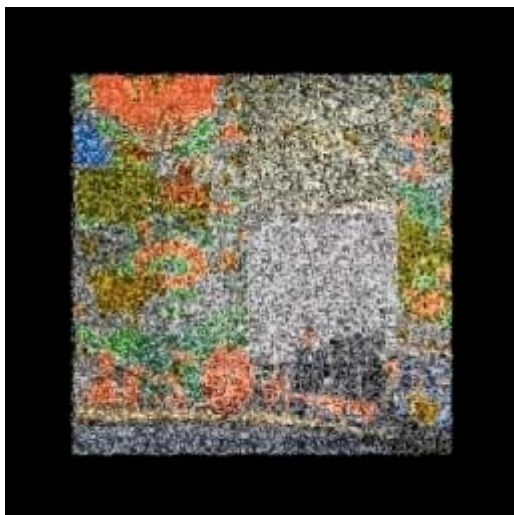


9. [frame_removed_video](#)



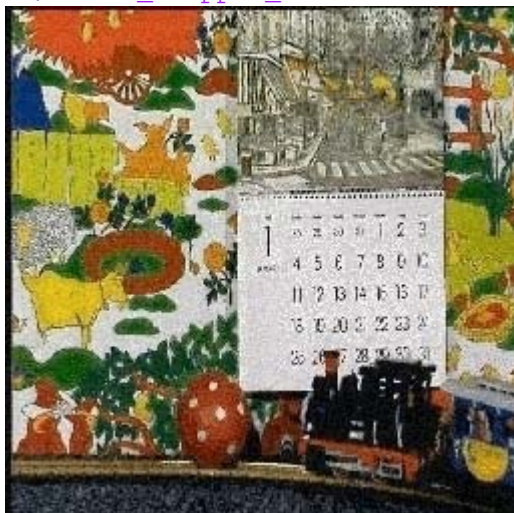


10. `frame_rotated_video`



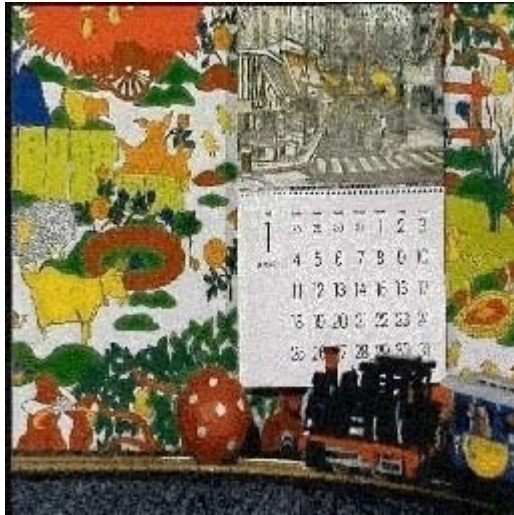


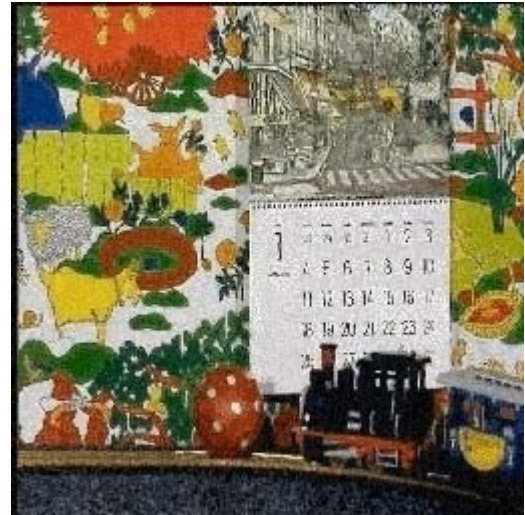
11. [frame_dropped_video](#)



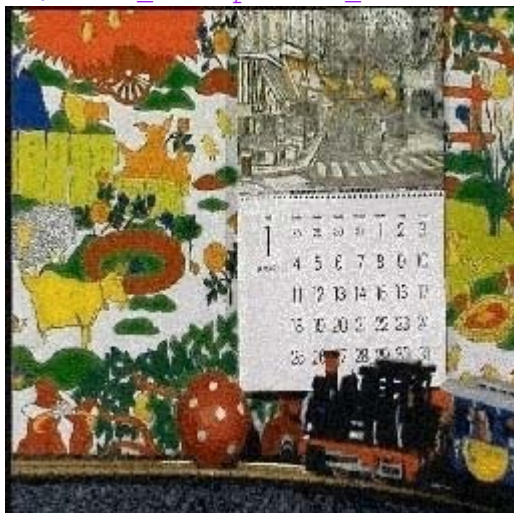


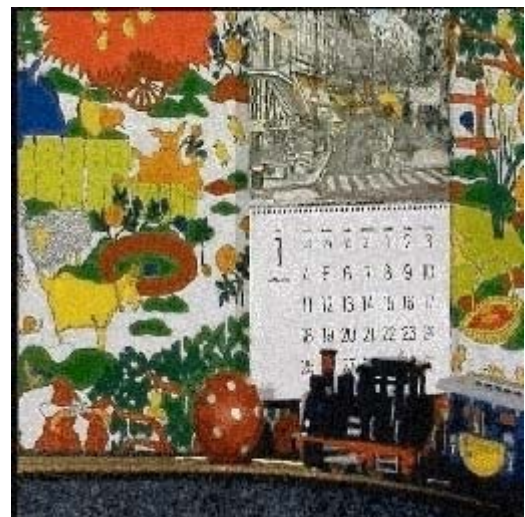
12. `frame_swapped_video`





13. [frame_interpolated_video](#)







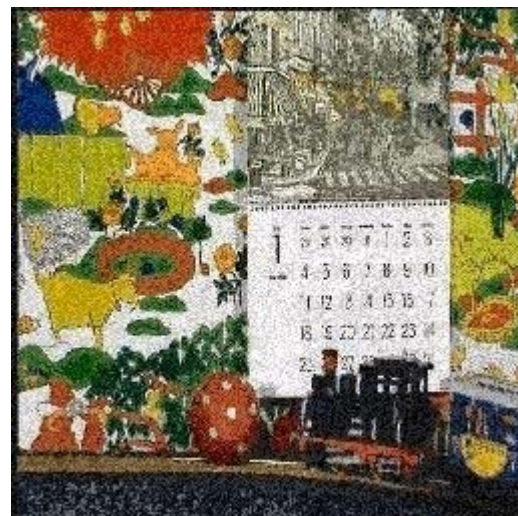
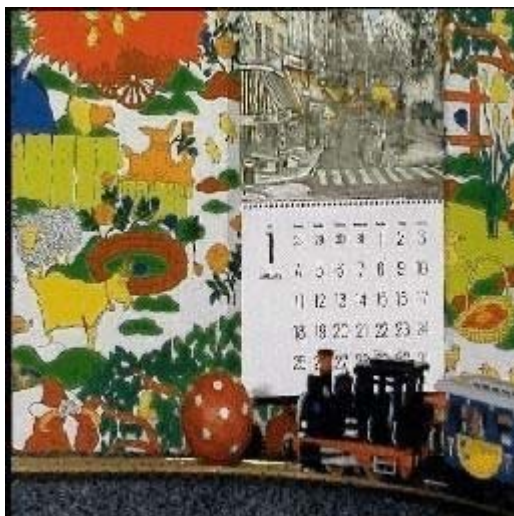
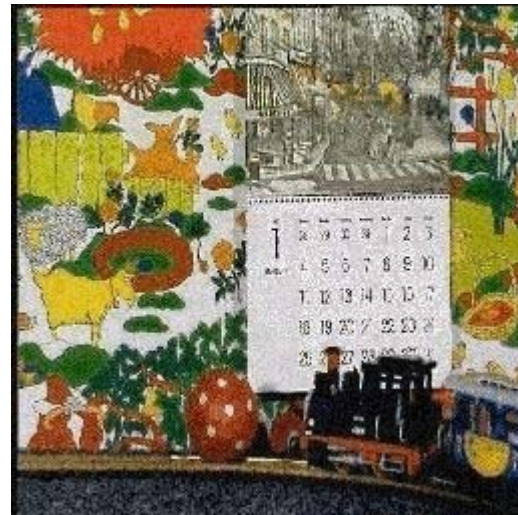
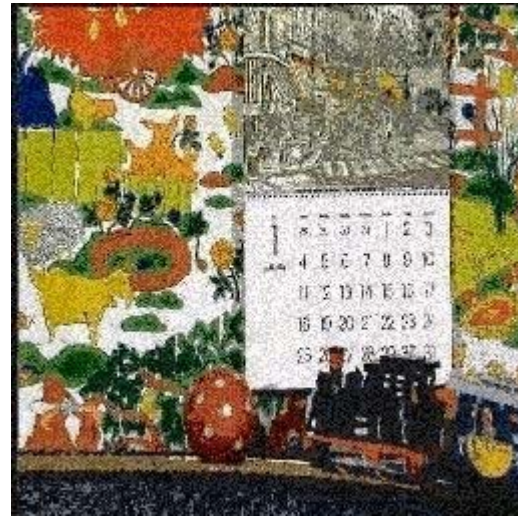
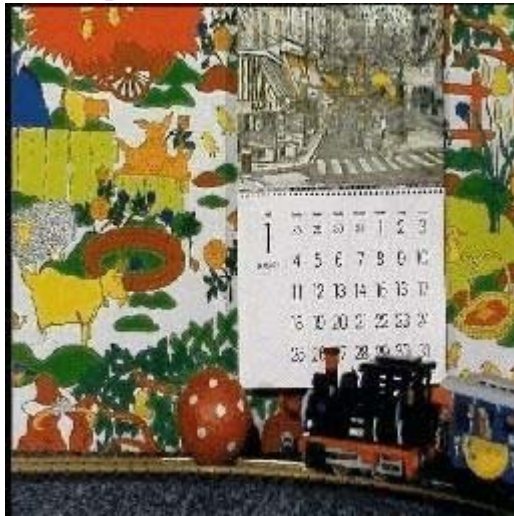
14. [frame_resized_video](#)

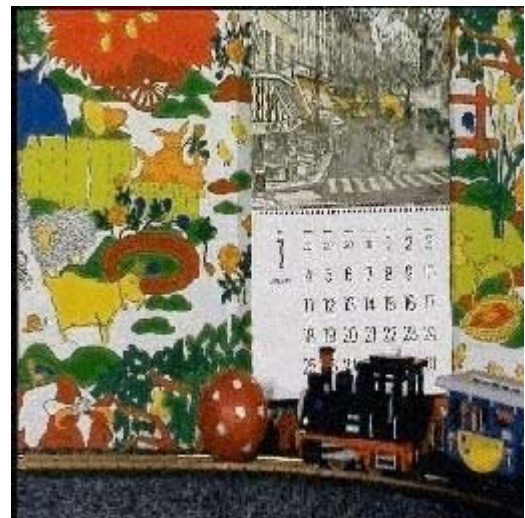
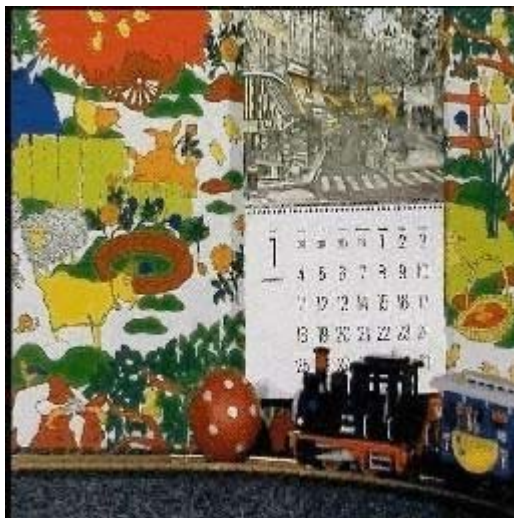
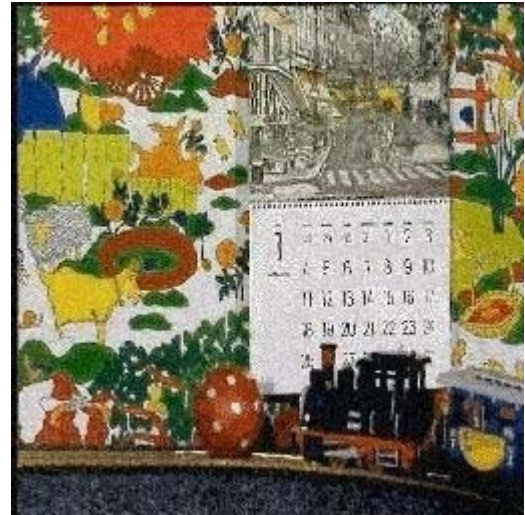
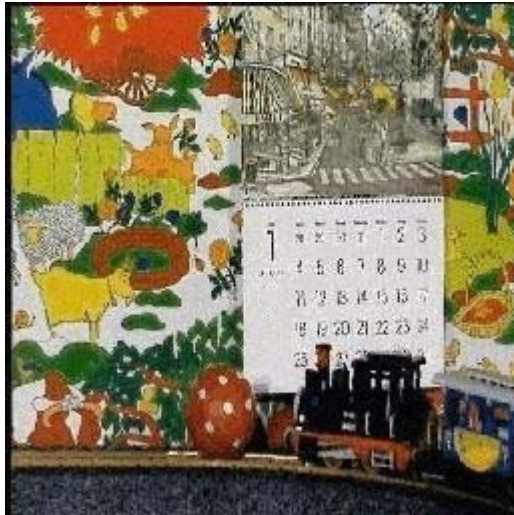




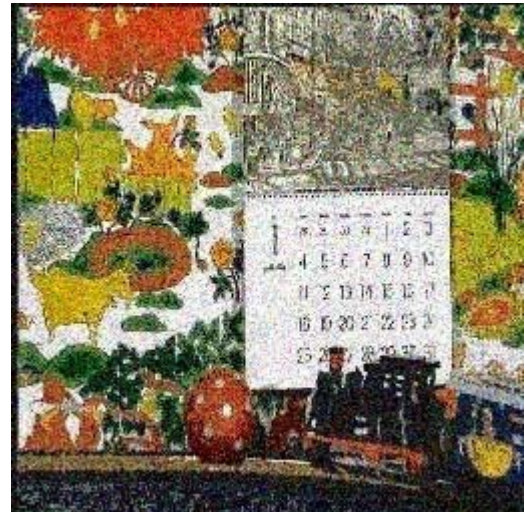
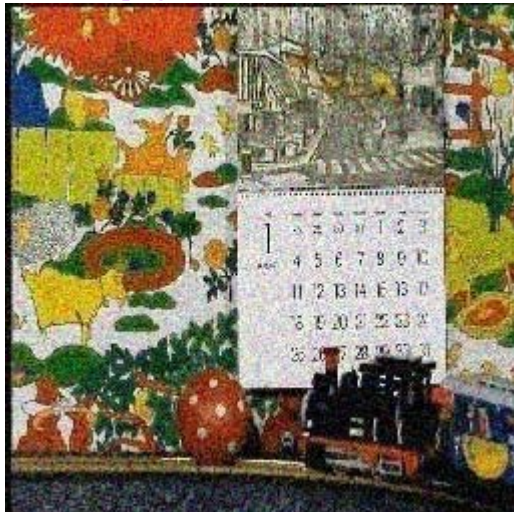
ATTACKED FRAMES
(WATERMARKING MID-SB PLANES)

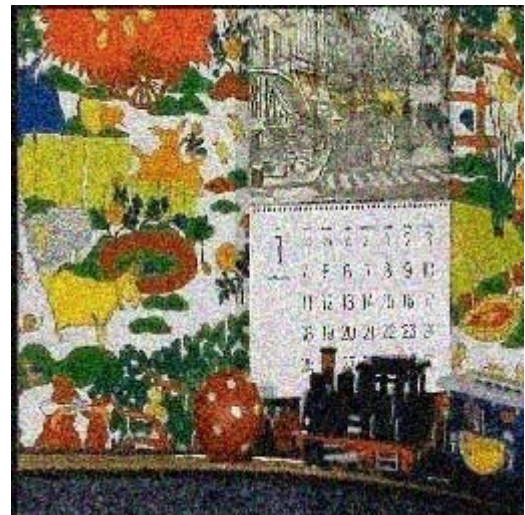
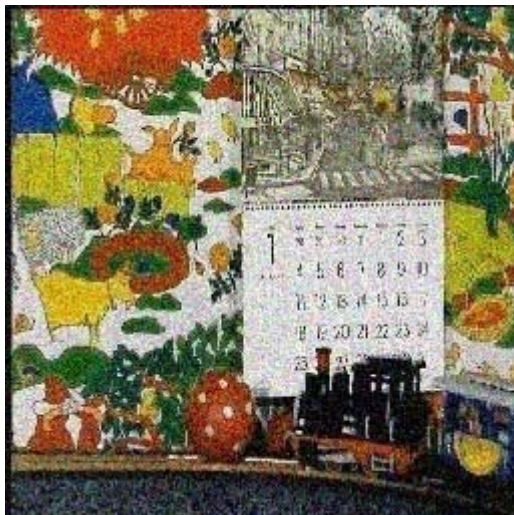
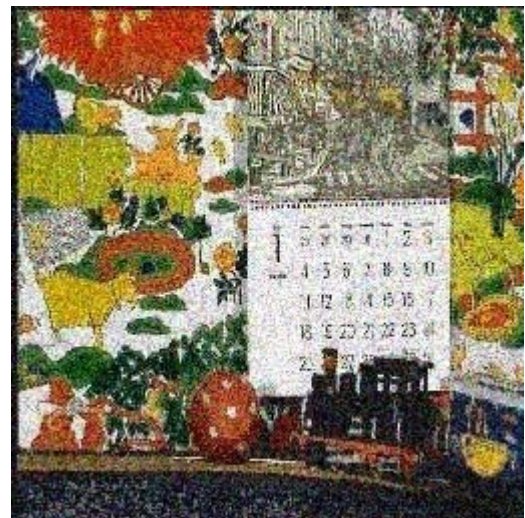
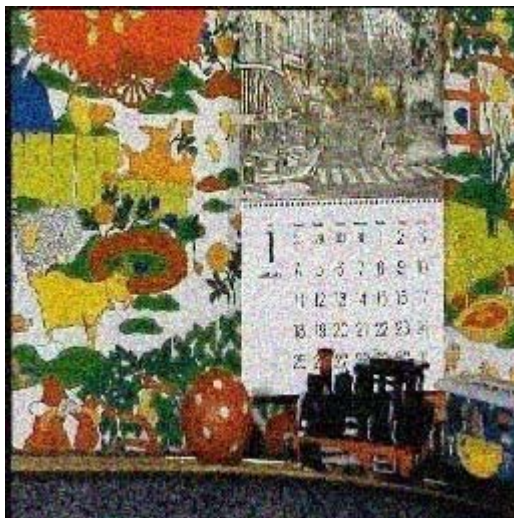
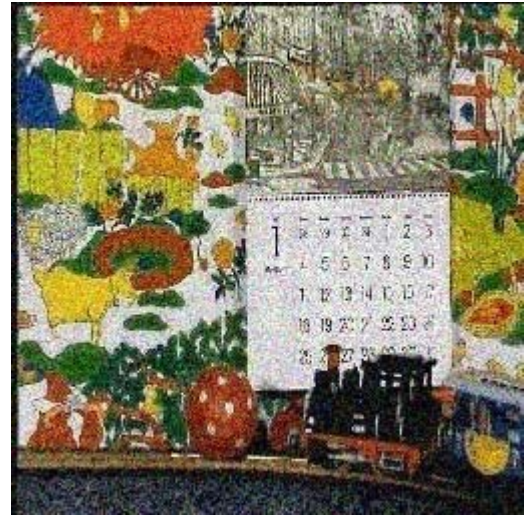
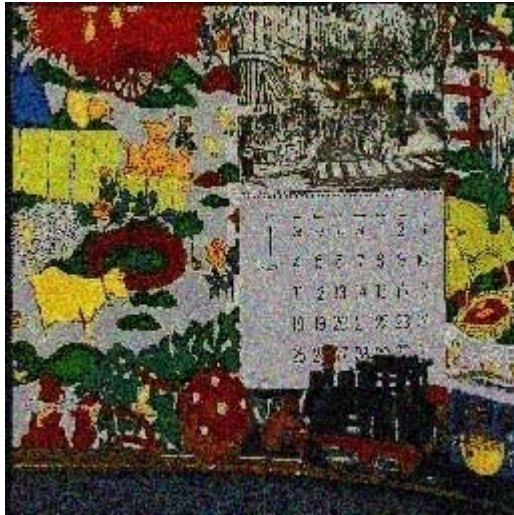
1. compressed video

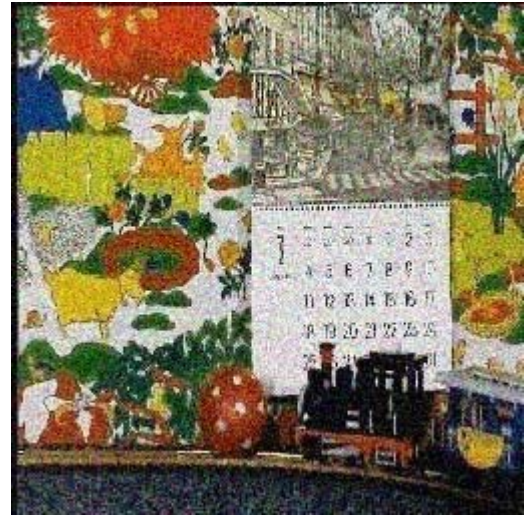
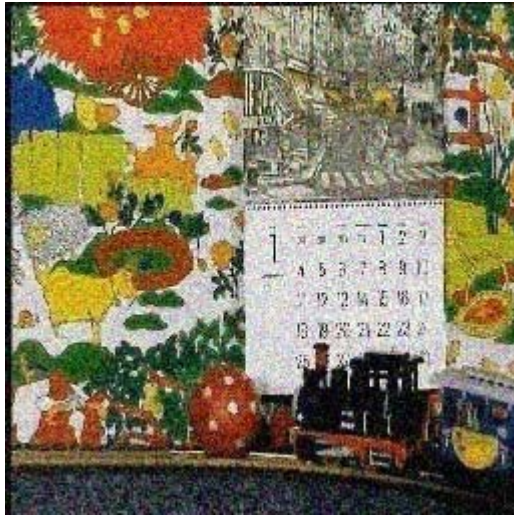




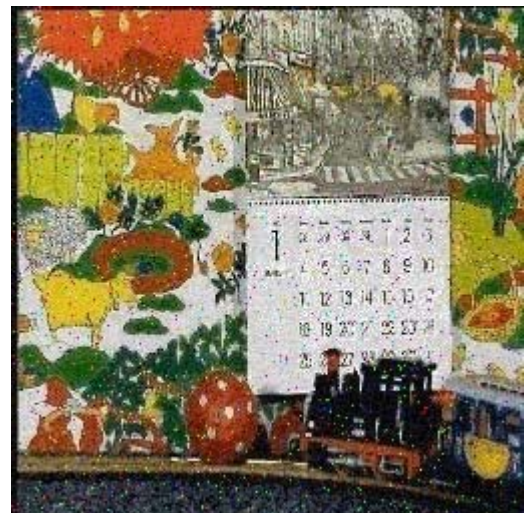
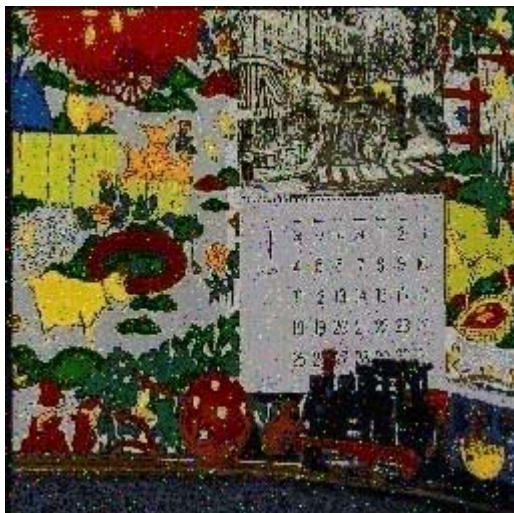
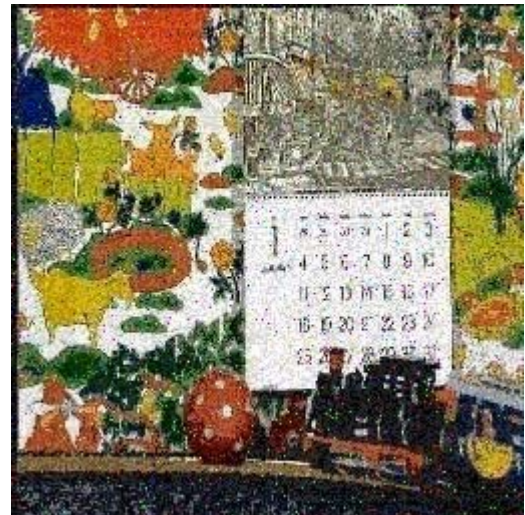
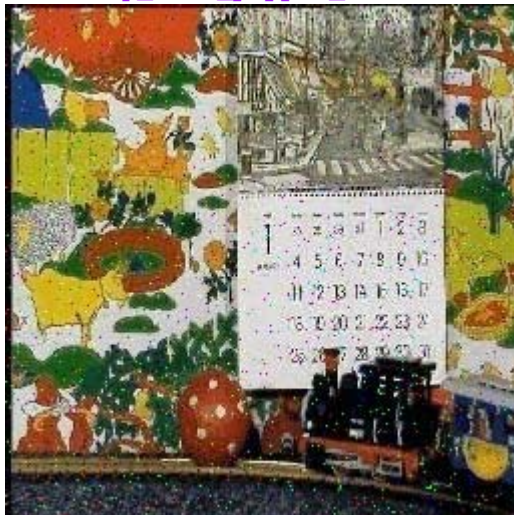
2. noisy_gaussian_video

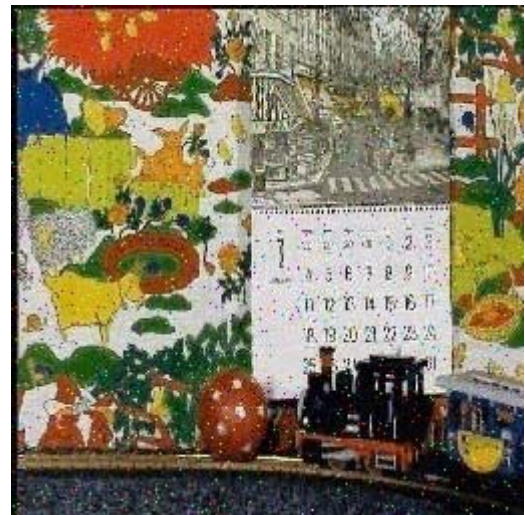
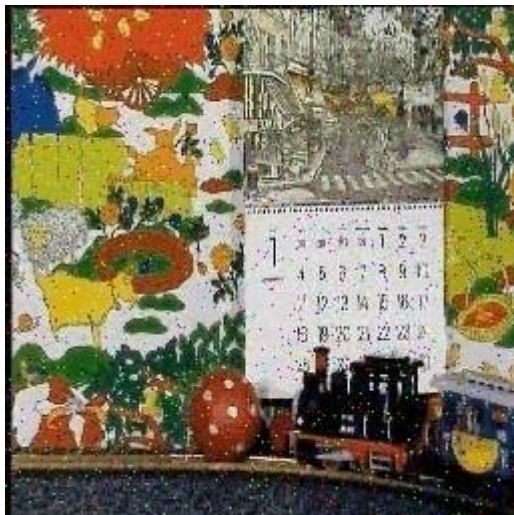
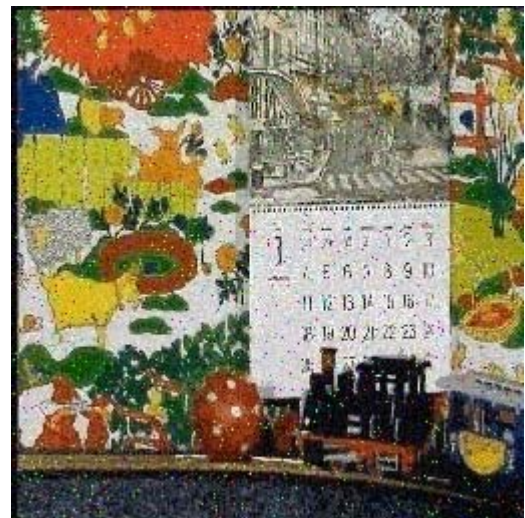
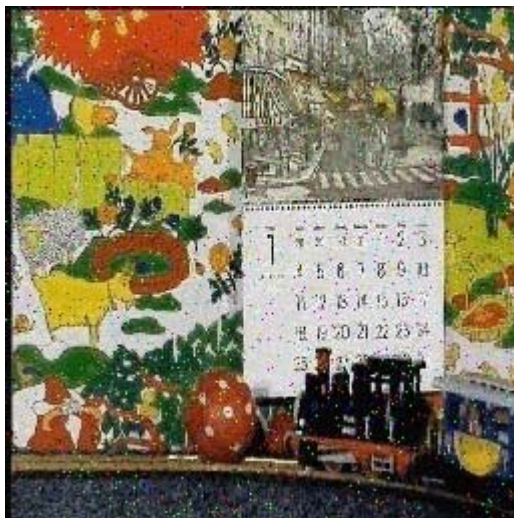
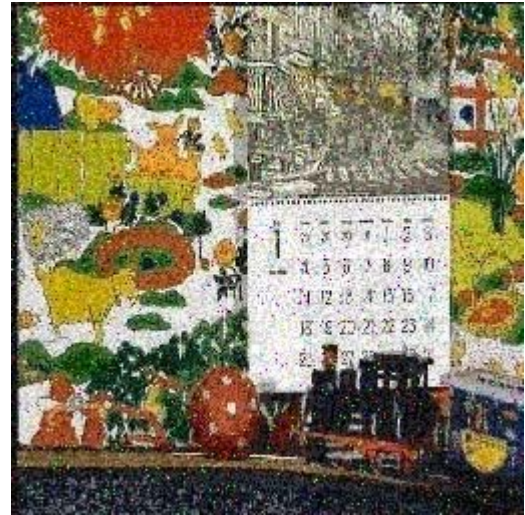
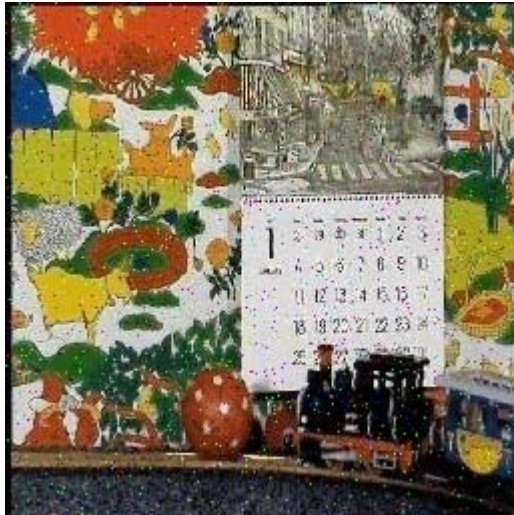






3. [noisy_salt_pepper_video](#)





4. averaged_filtered_video





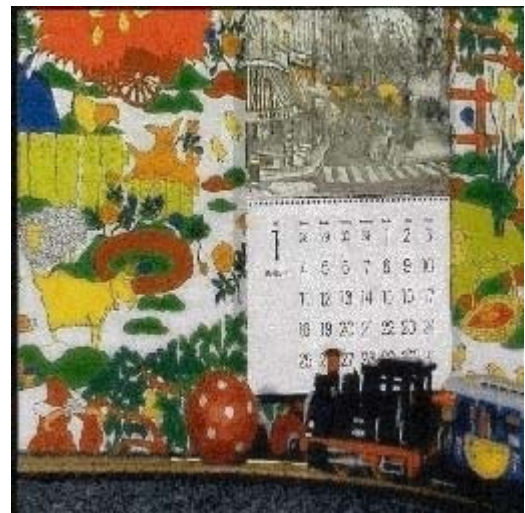
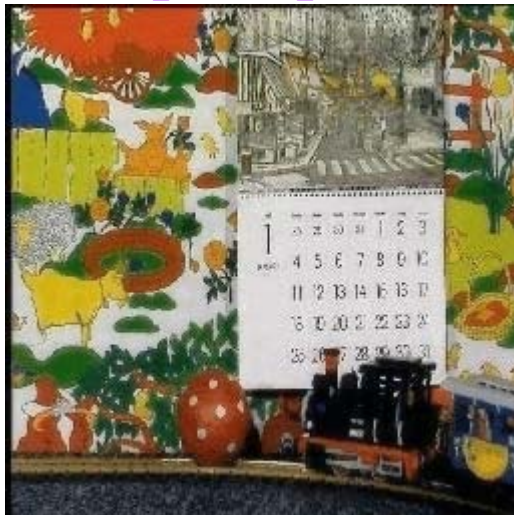
5. [median_filtered_video](#)

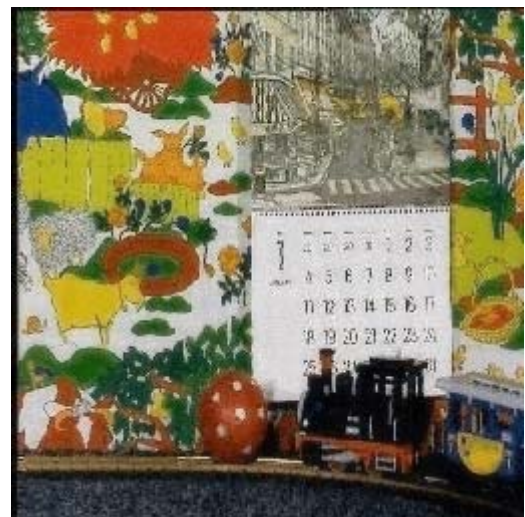
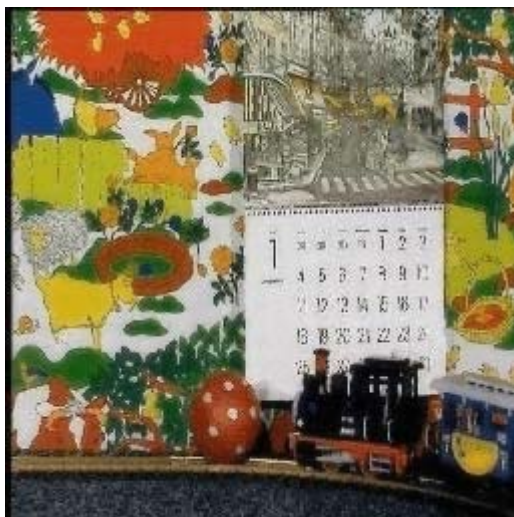
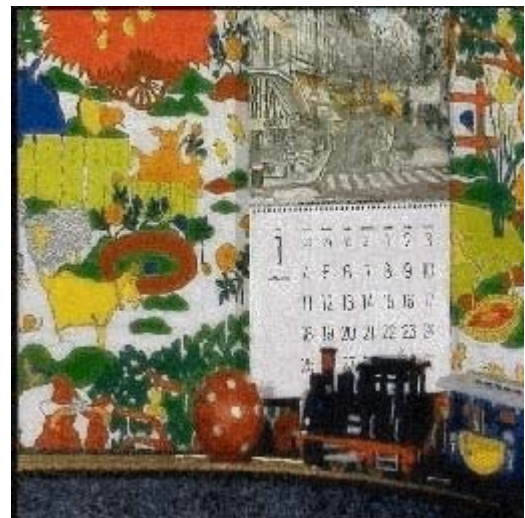
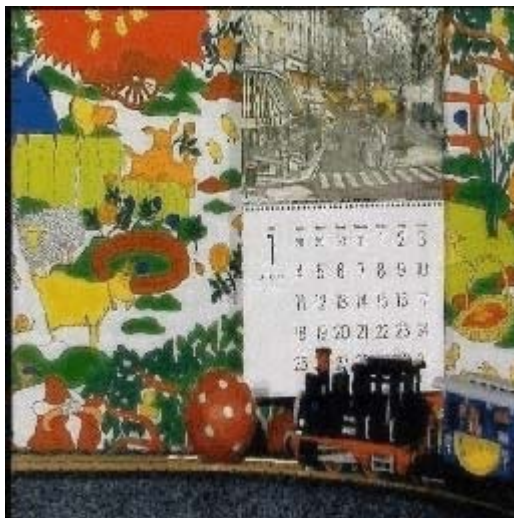




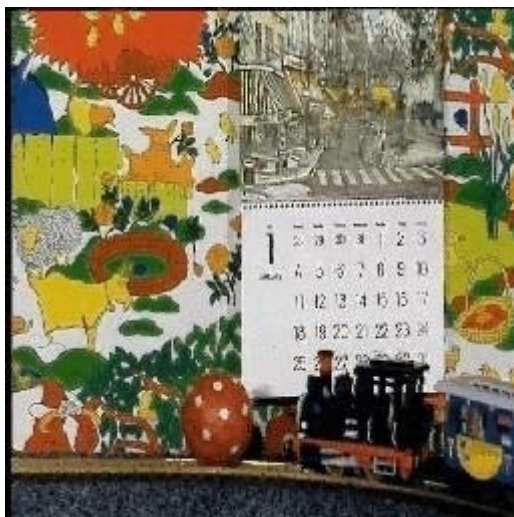
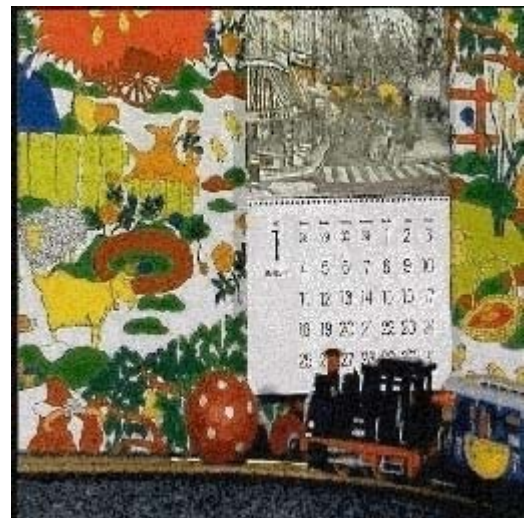
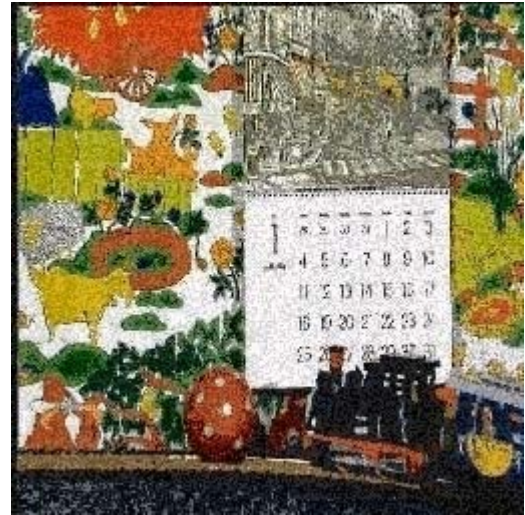
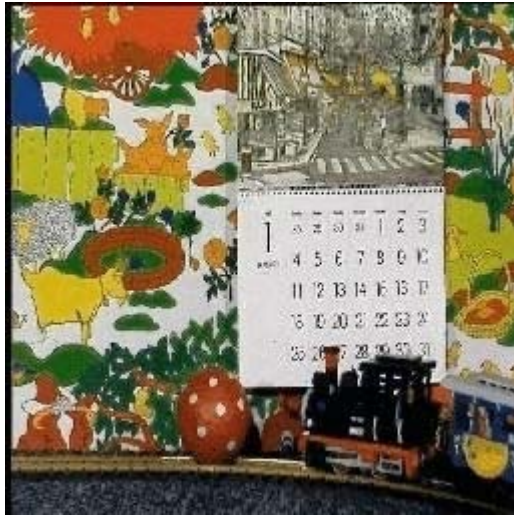


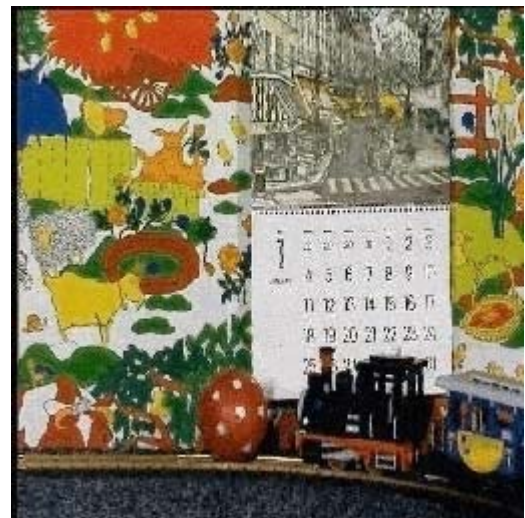
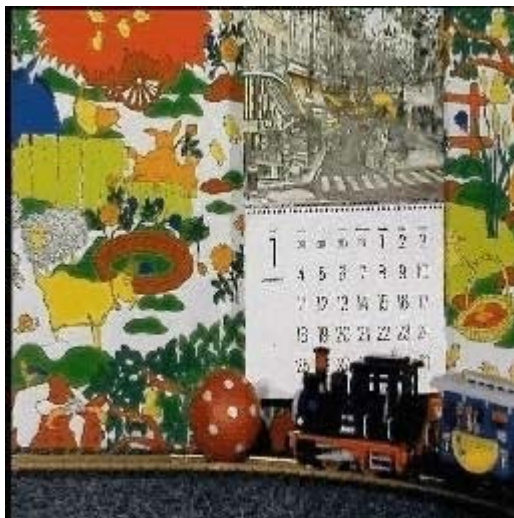
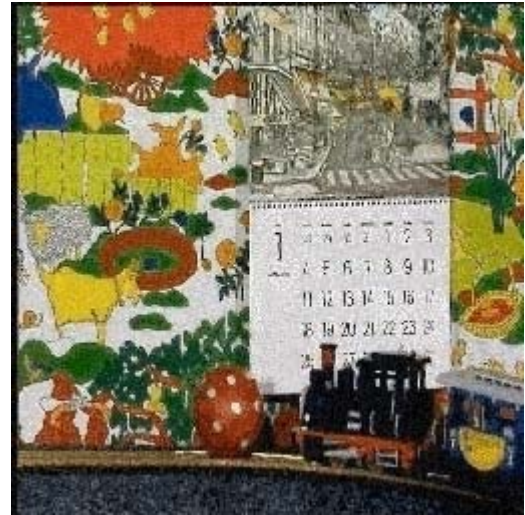
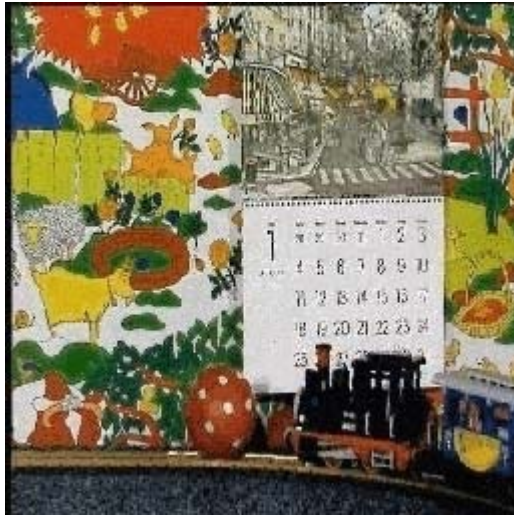
6. wiener_filtered_video



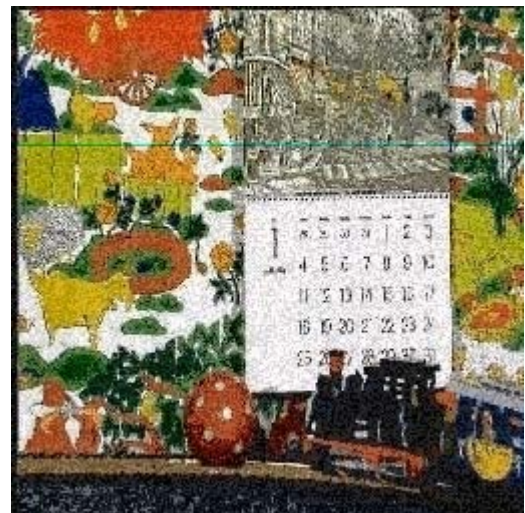
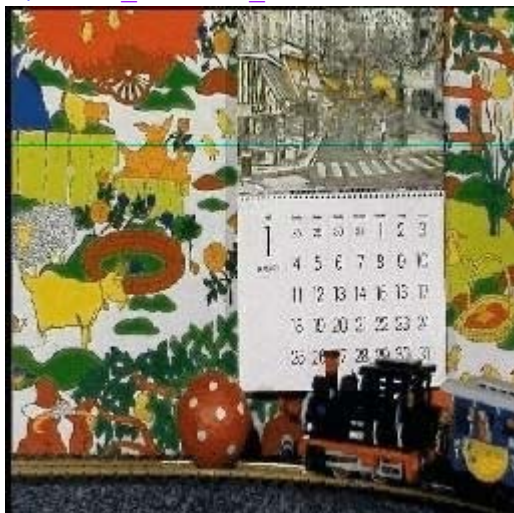


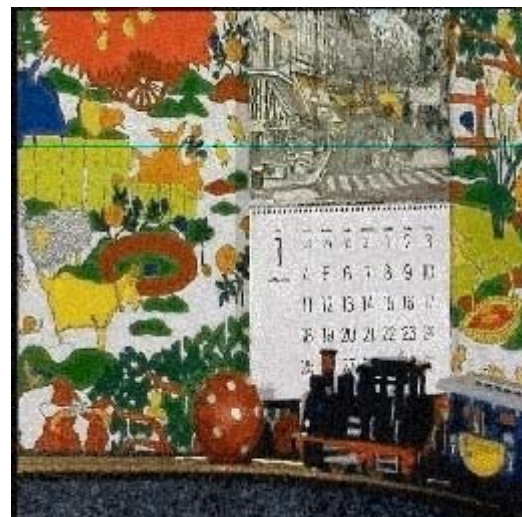
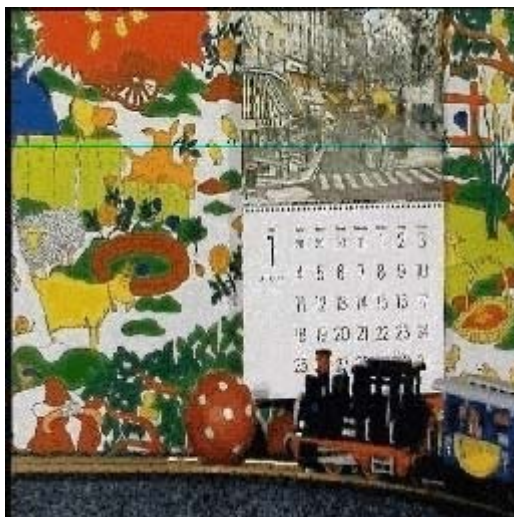
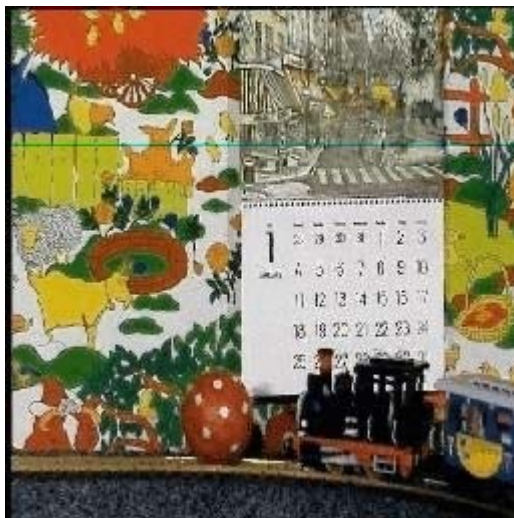
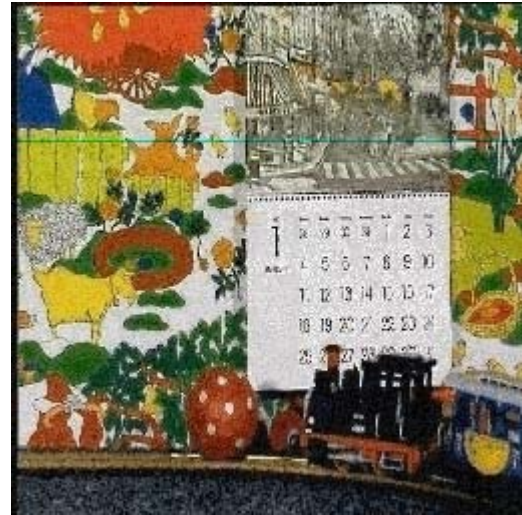
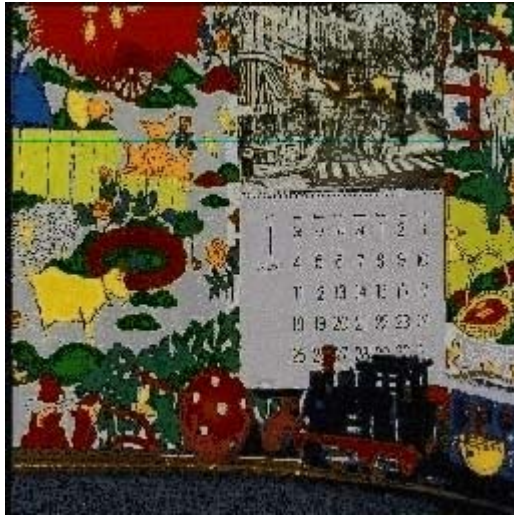
7. `pixel_removed_video`





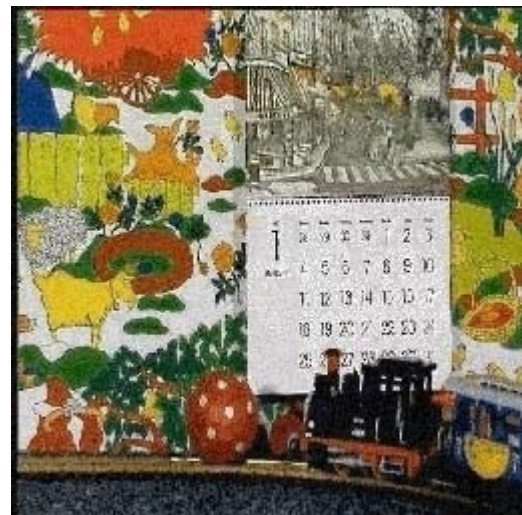
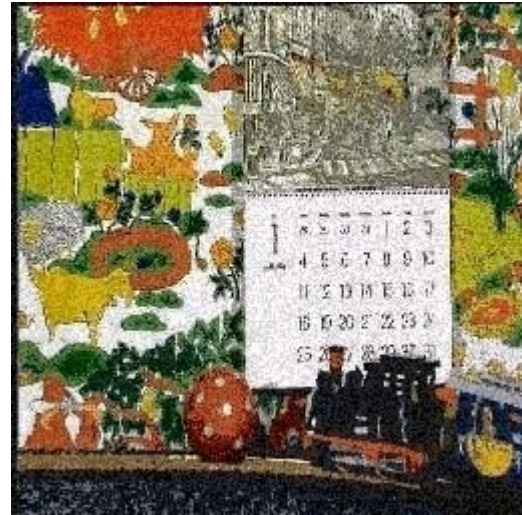
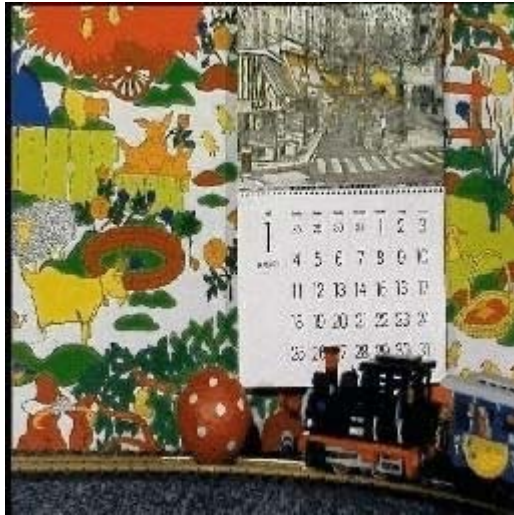
8. [line_removed_video](#)

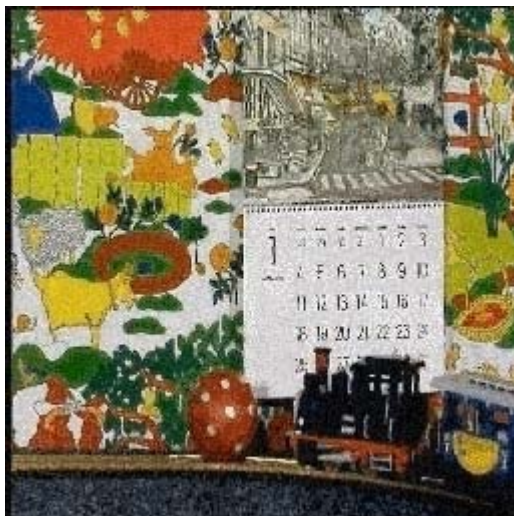
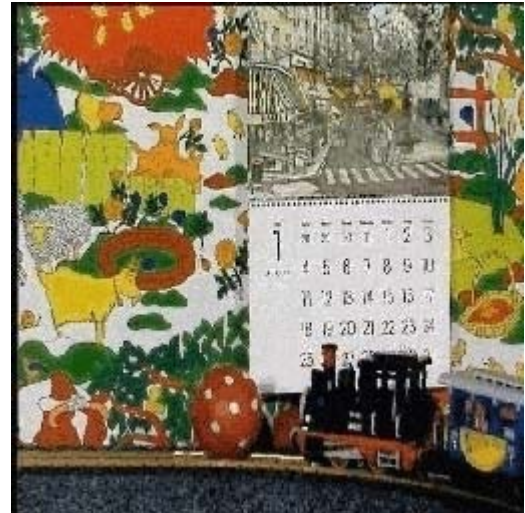






9. `frame_removed_video`





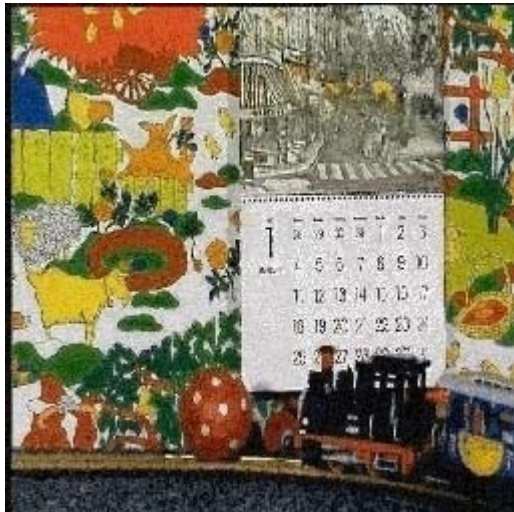
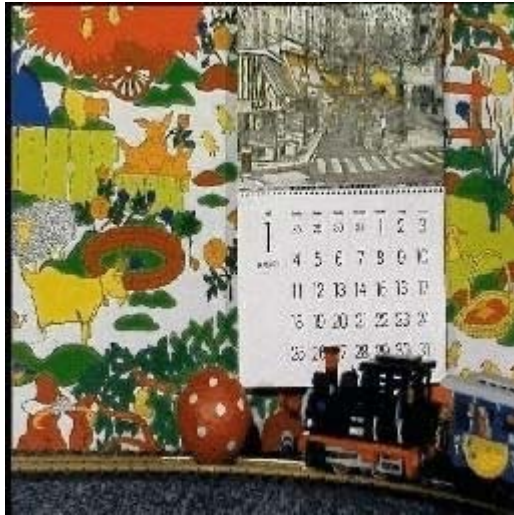
10. [frame_rotated_video](#)

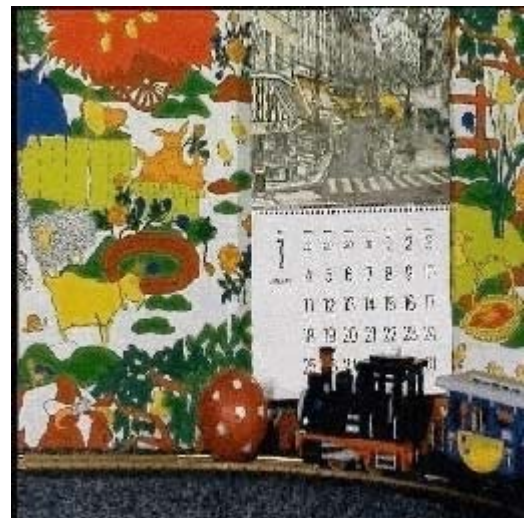
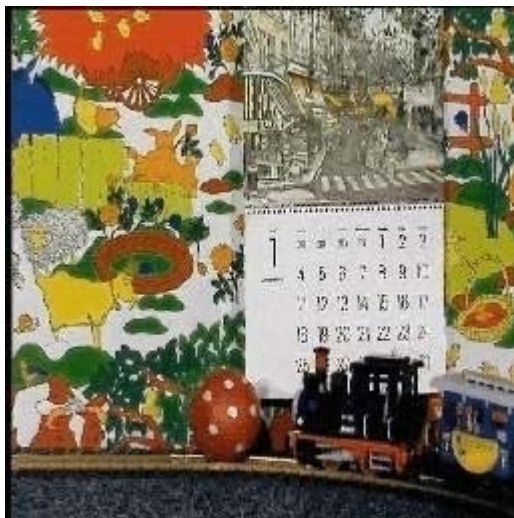
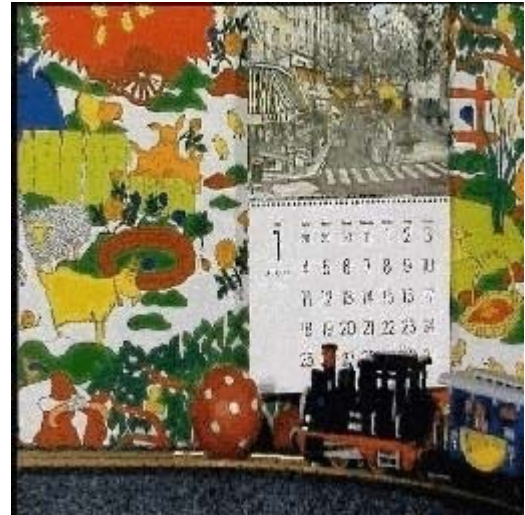




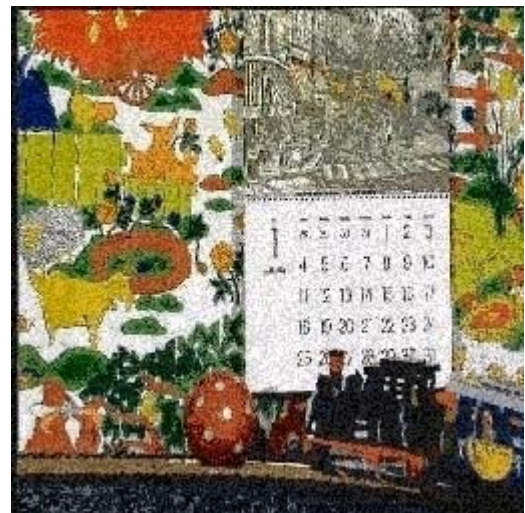
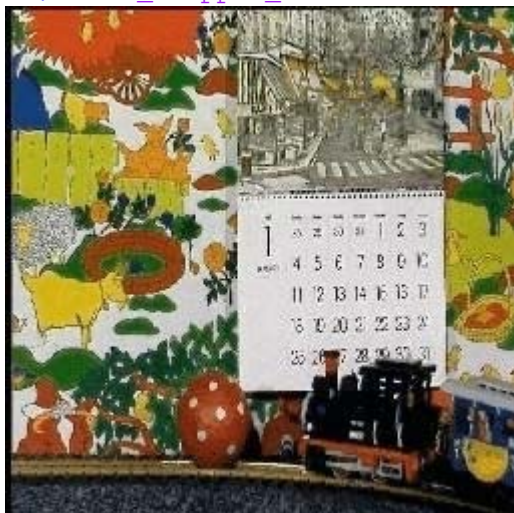


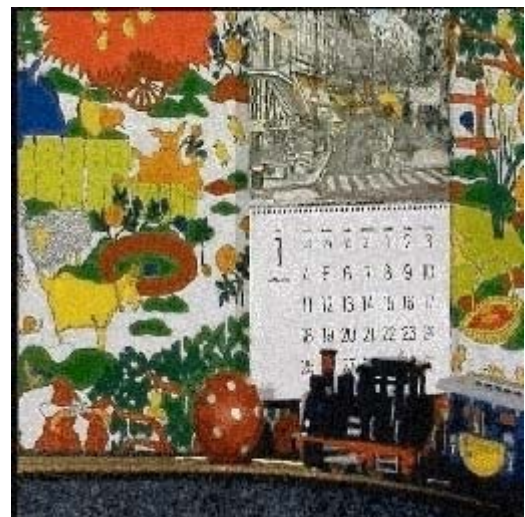
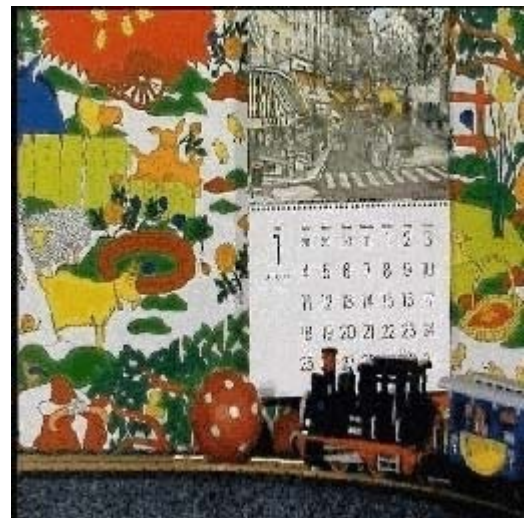
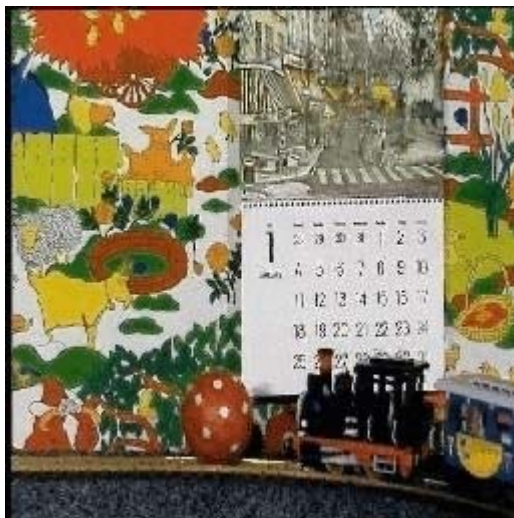
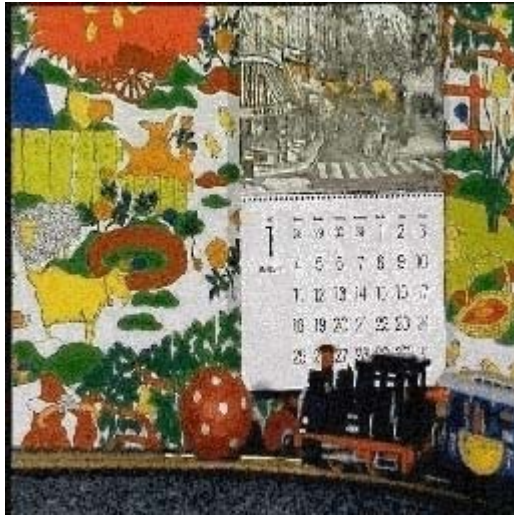
11. [frame_dropped_video](#)

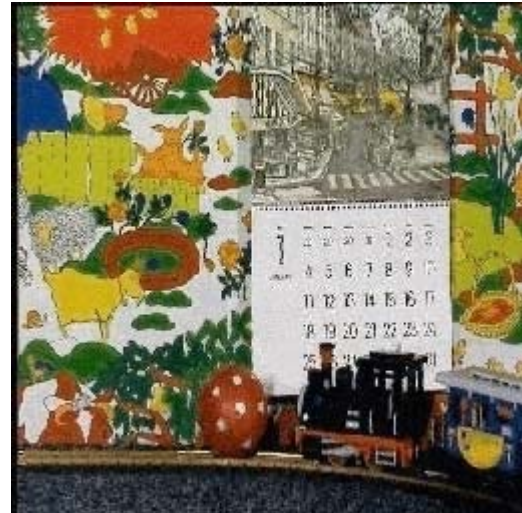




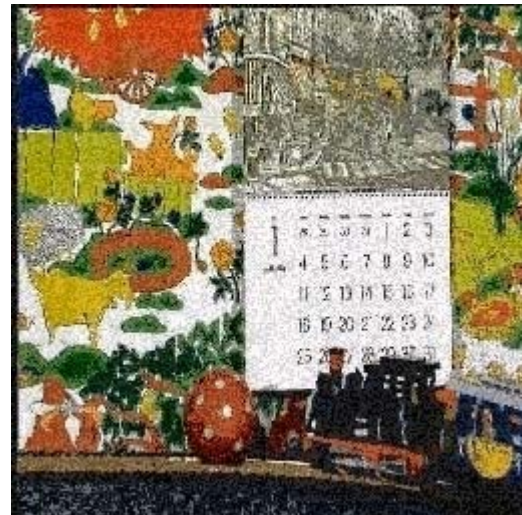
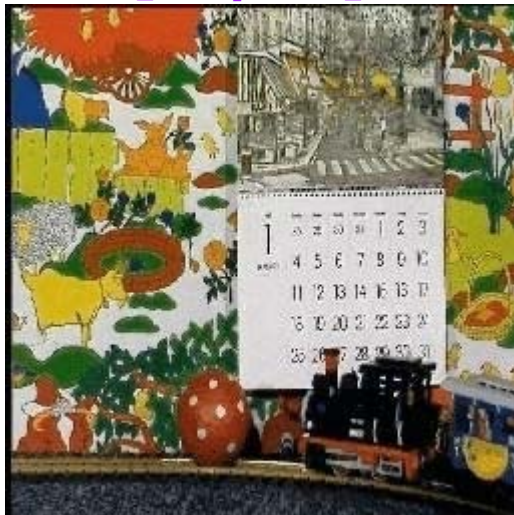
12. frame_swapped_video

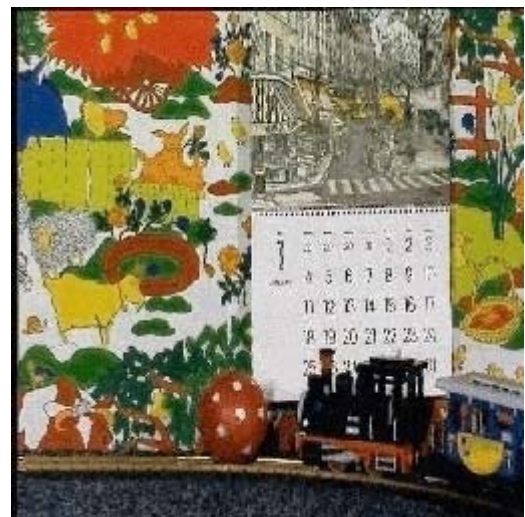
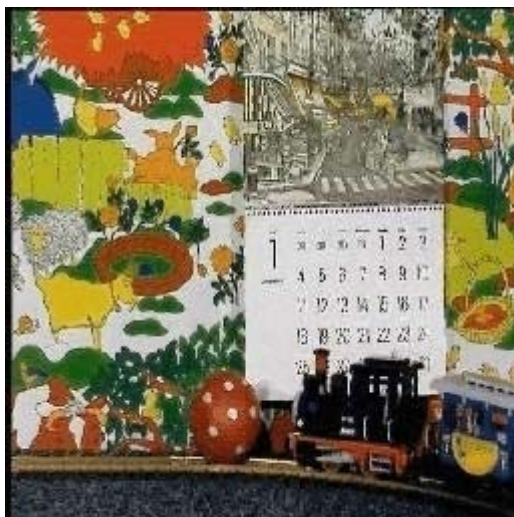
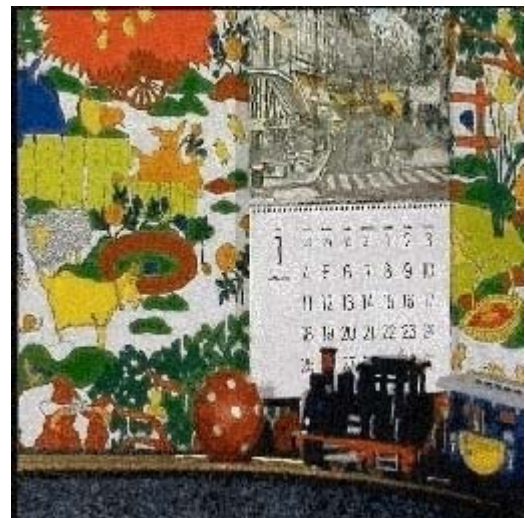






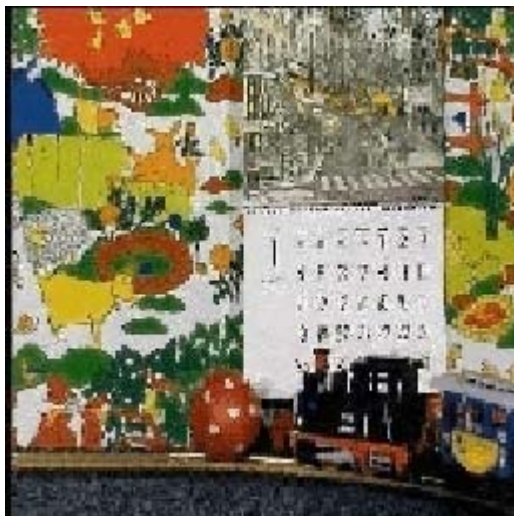
13. frame_interpolated_video





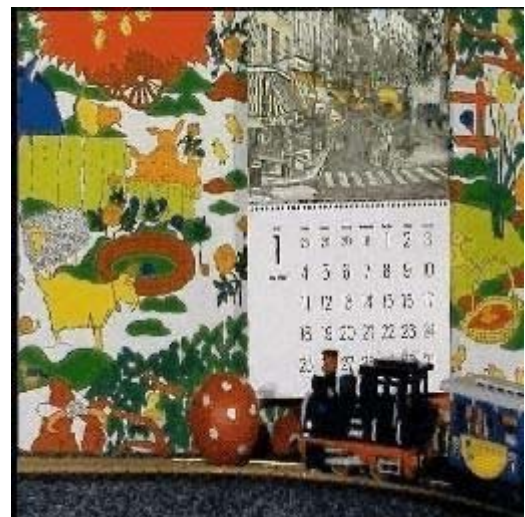
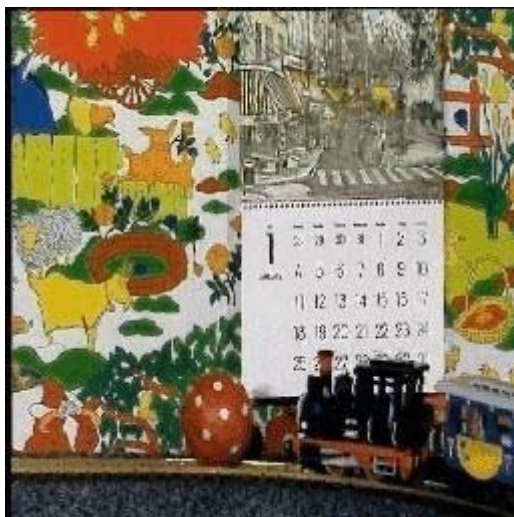
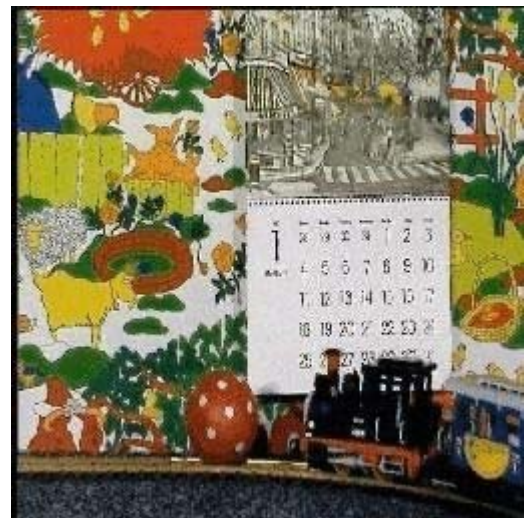
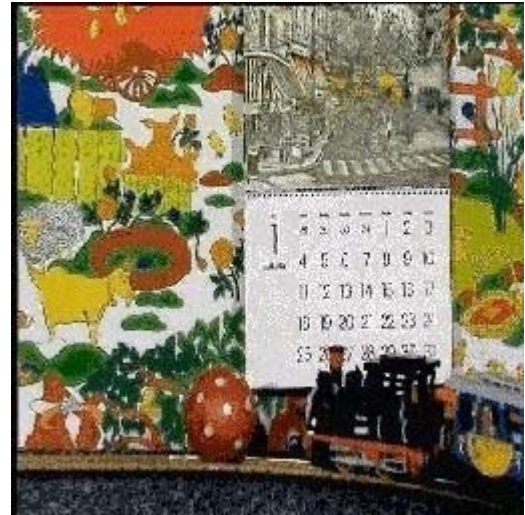
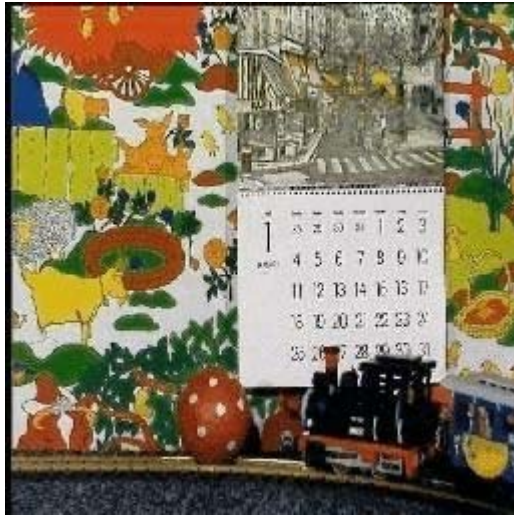
14. `frame_resized_video`

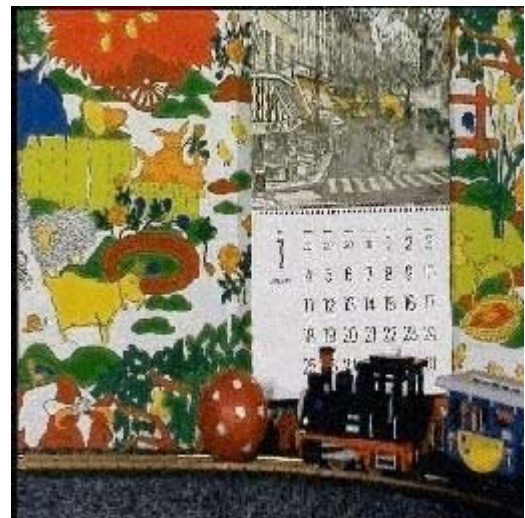
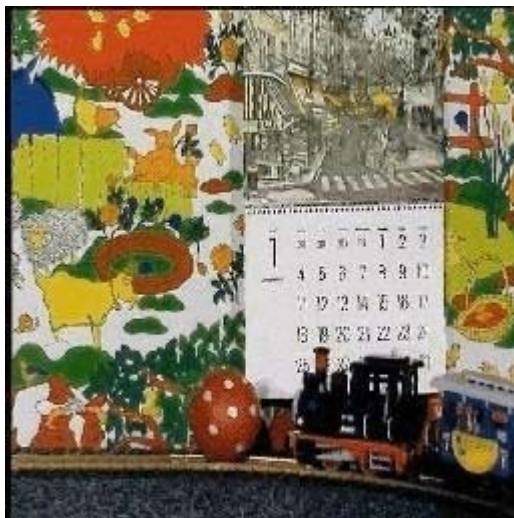
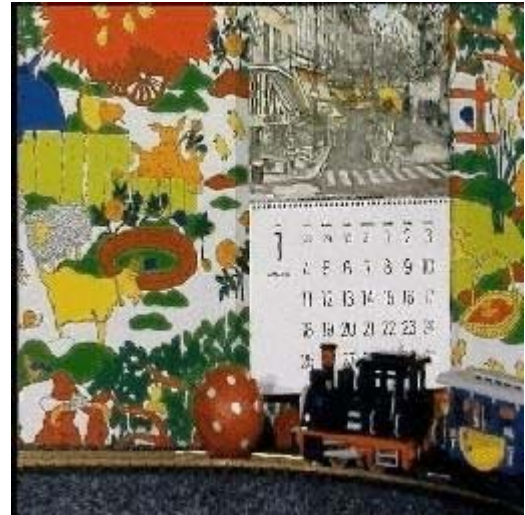
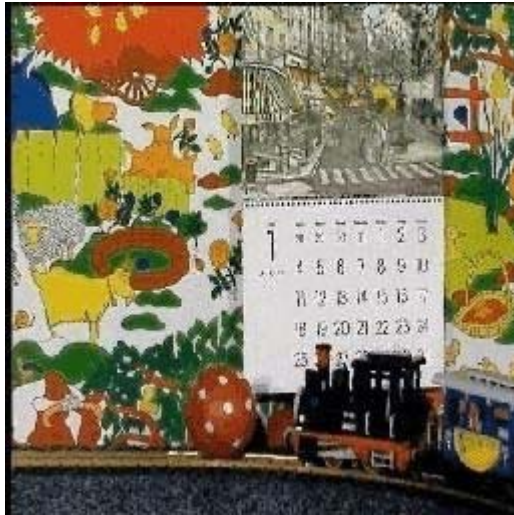




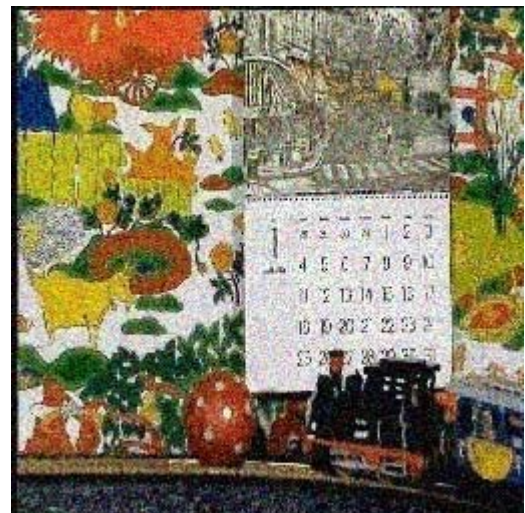
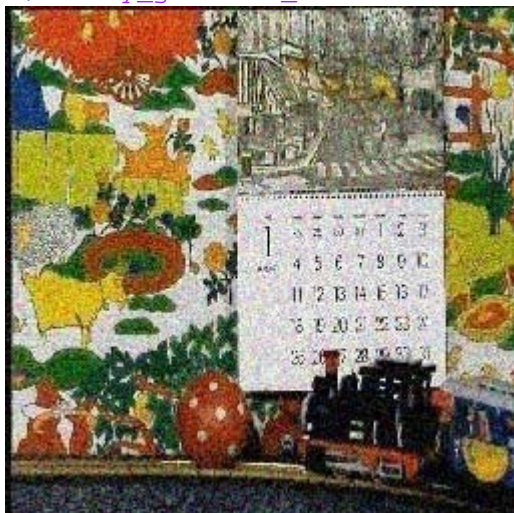
ATTACKED FRAMES
(WATERMARKING LSB PLANES)

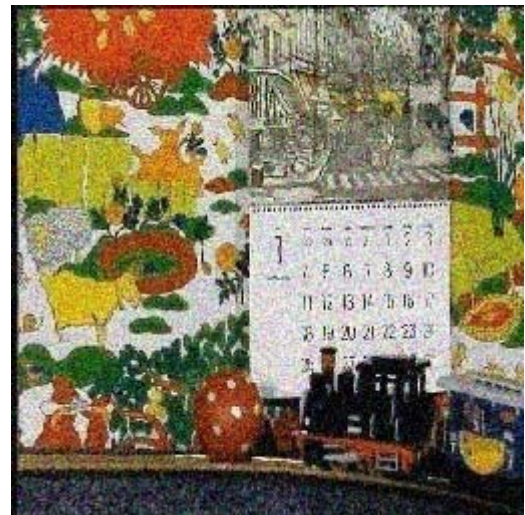
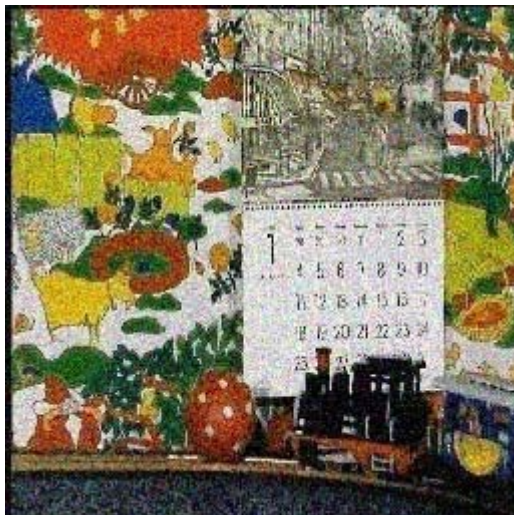
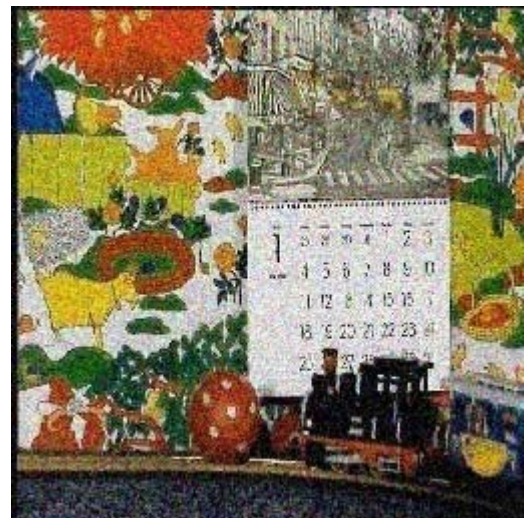
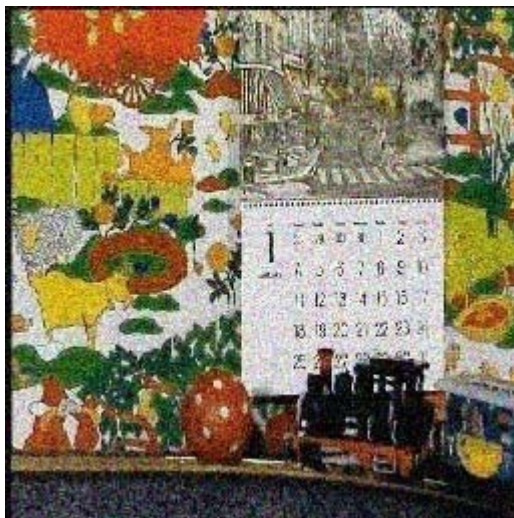
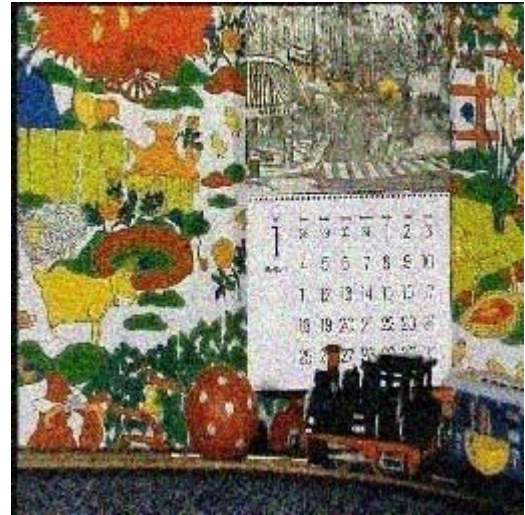
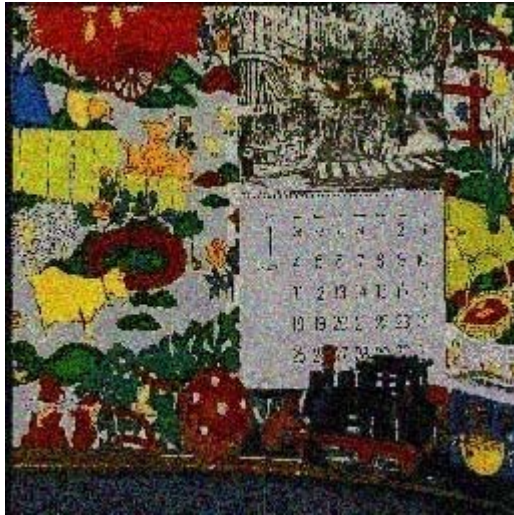
1. `compressed_video`

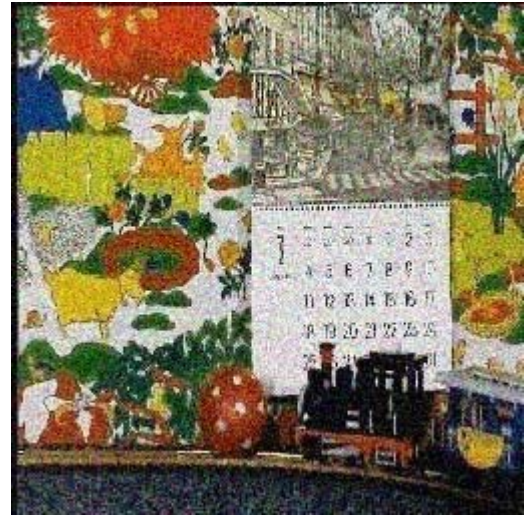
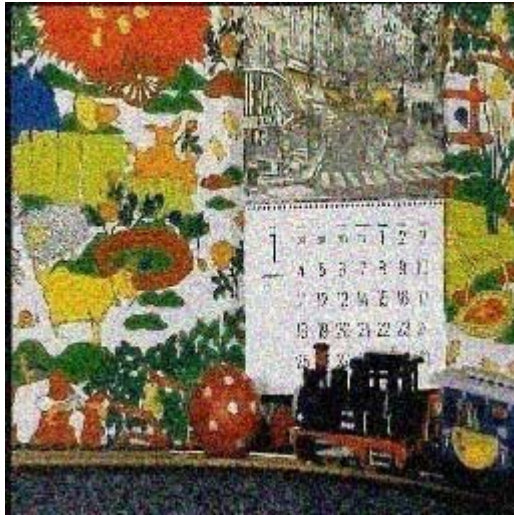




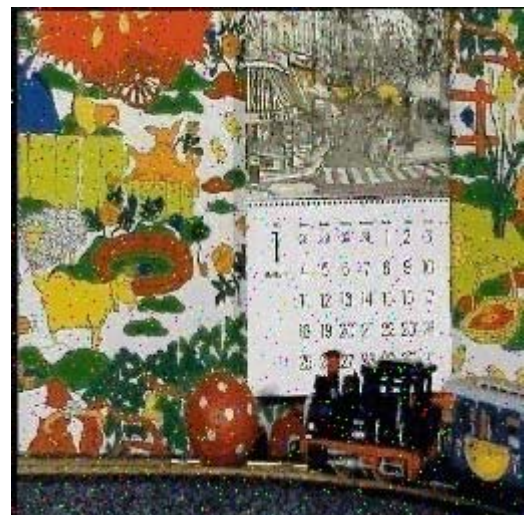
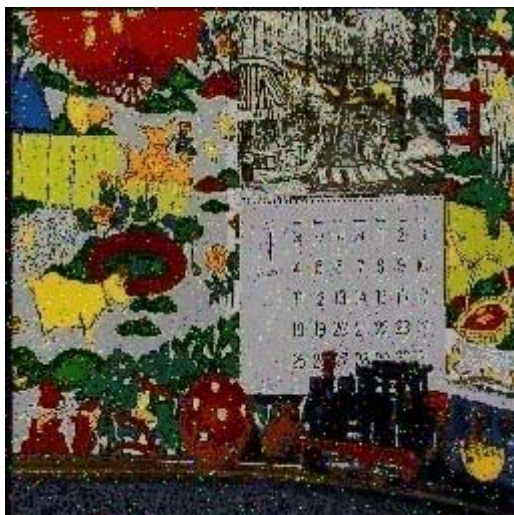
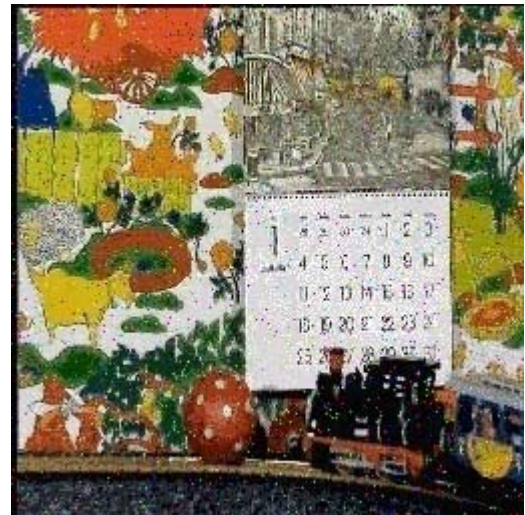
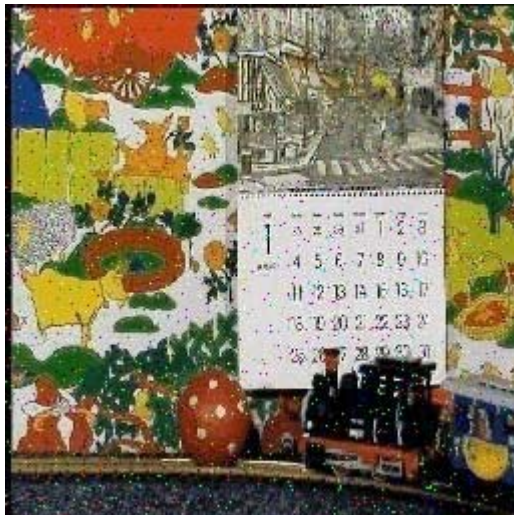
2. noisy_gaussian_video

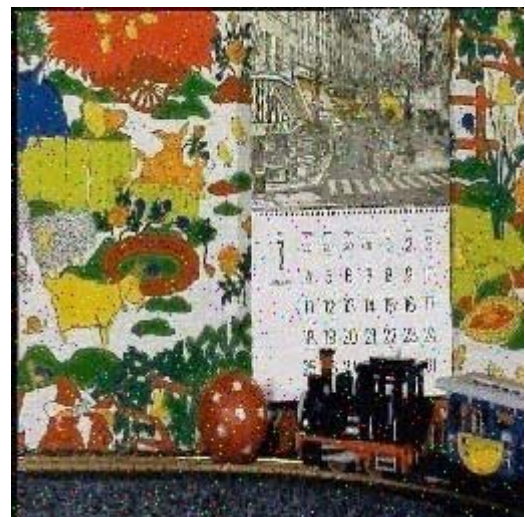
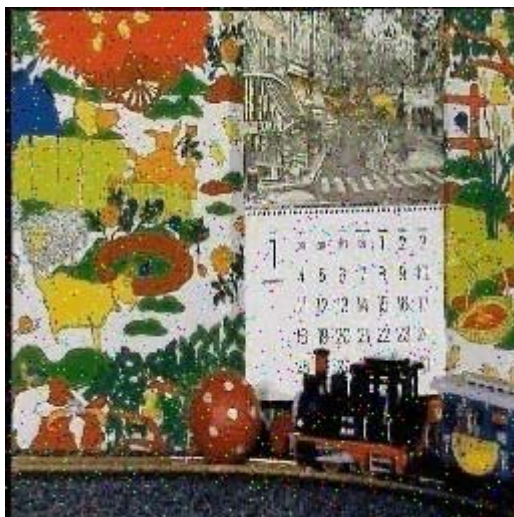
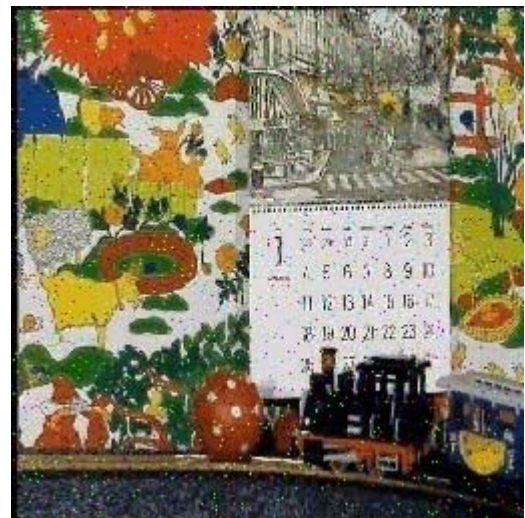
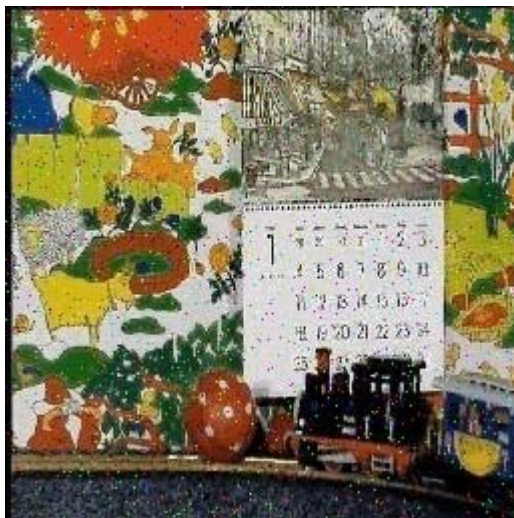
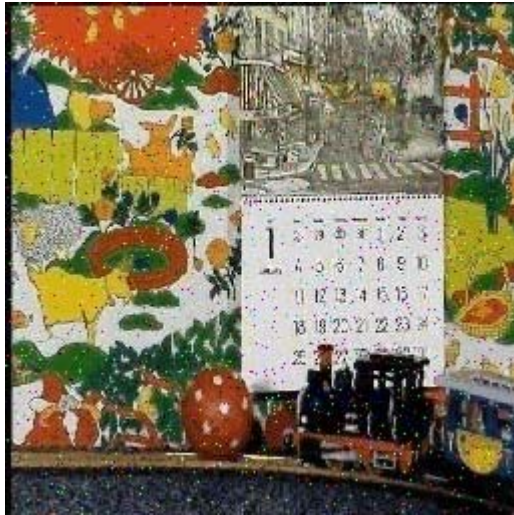






3. noisy_salt_pepper_video





4. `averaged_filtered_video`





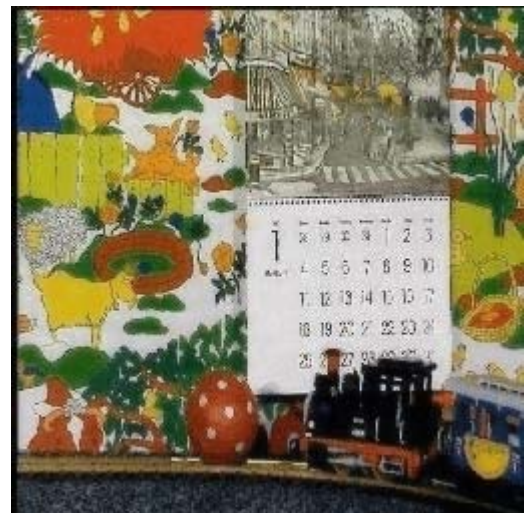
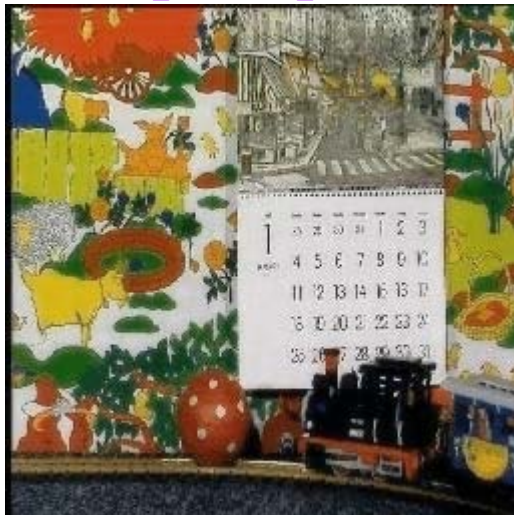
5. [median_filtered_video](#)

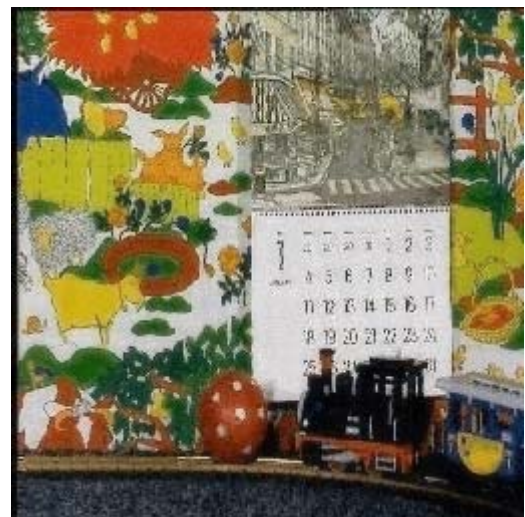
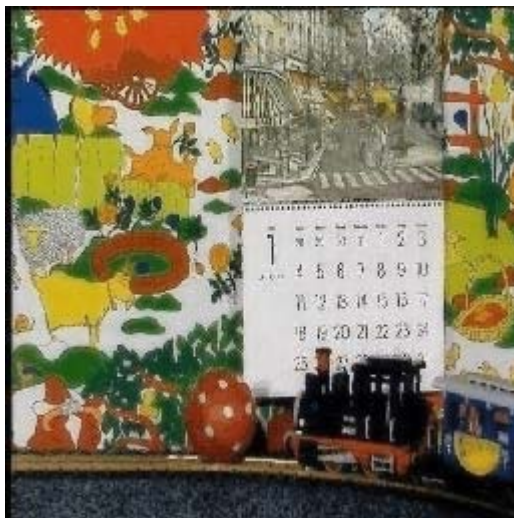




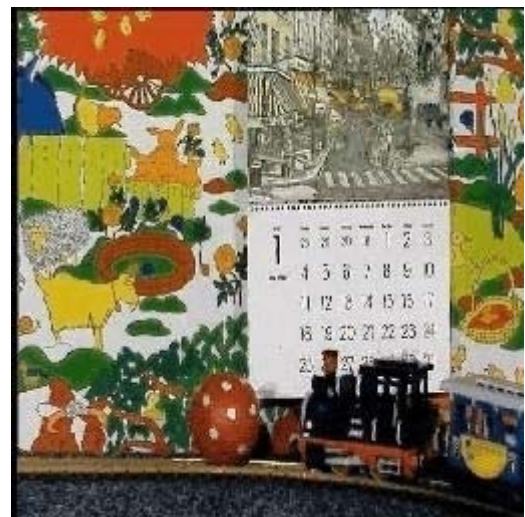
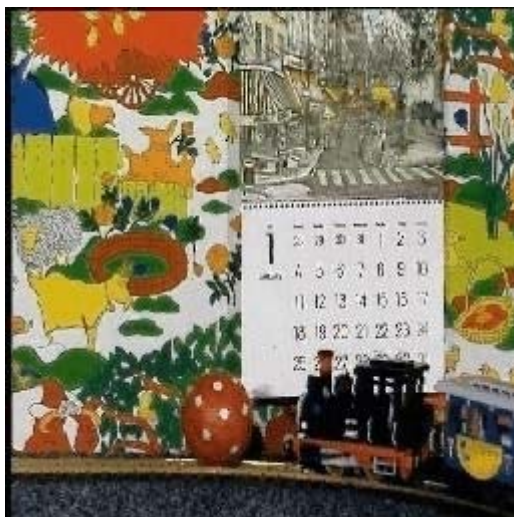
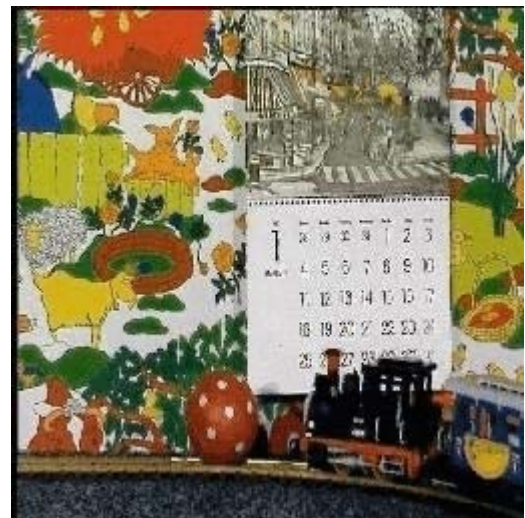
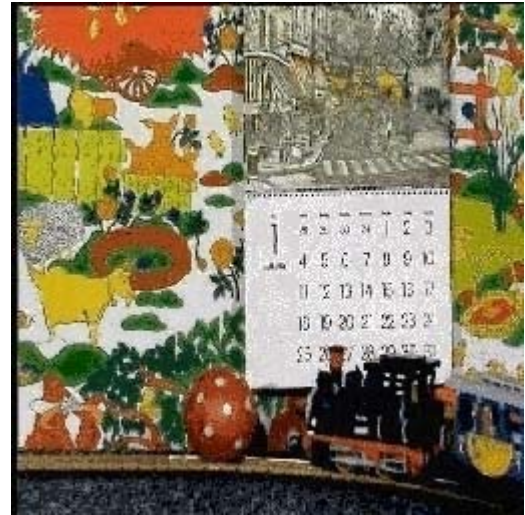


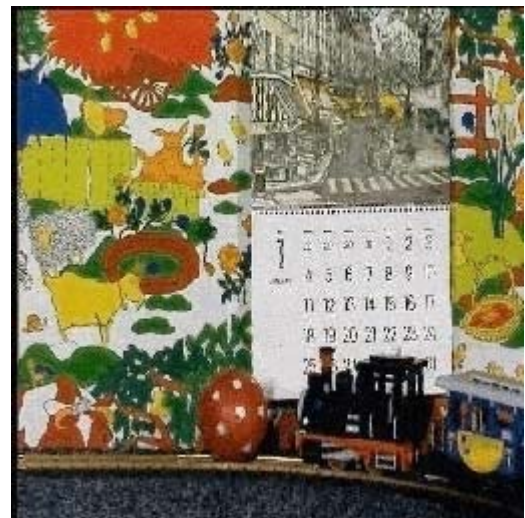
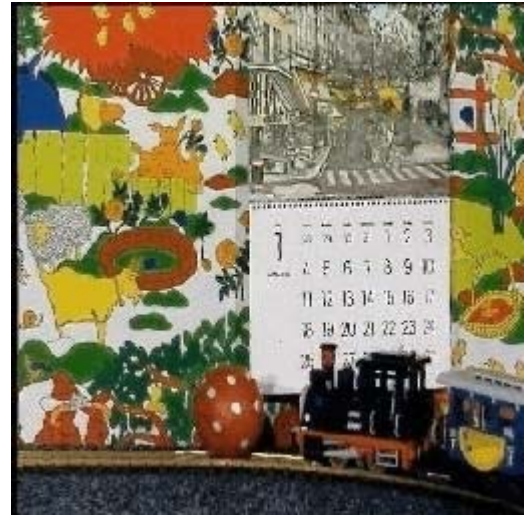
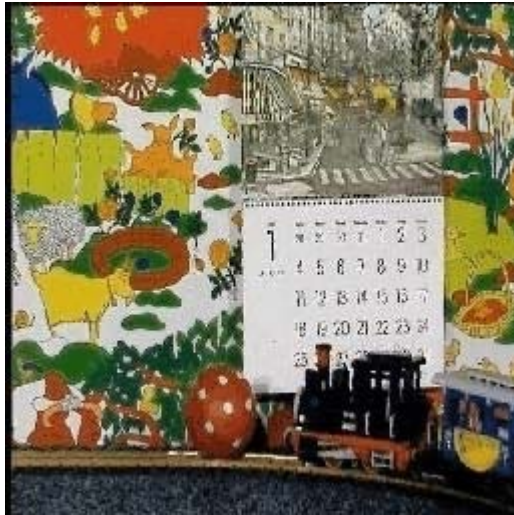
6. wiener_filtered_video



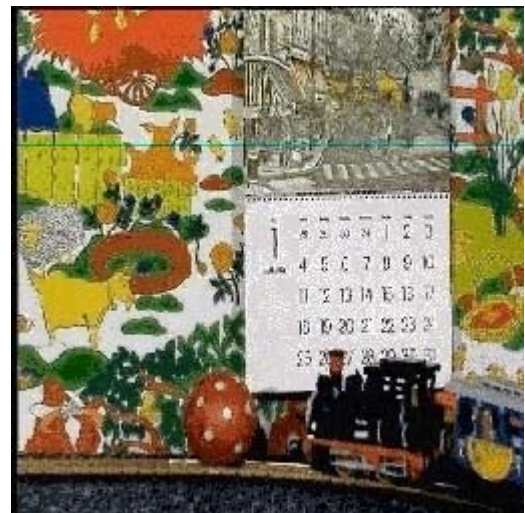
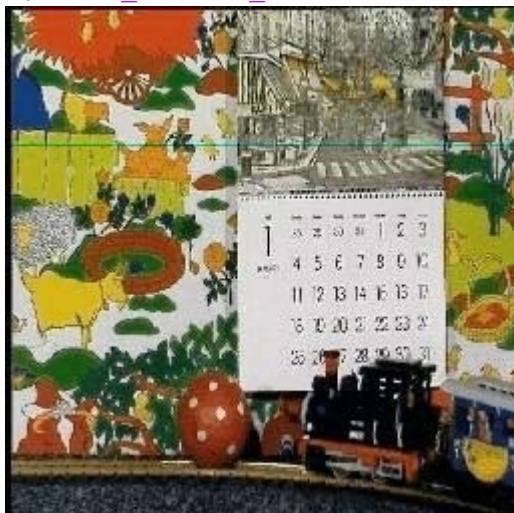


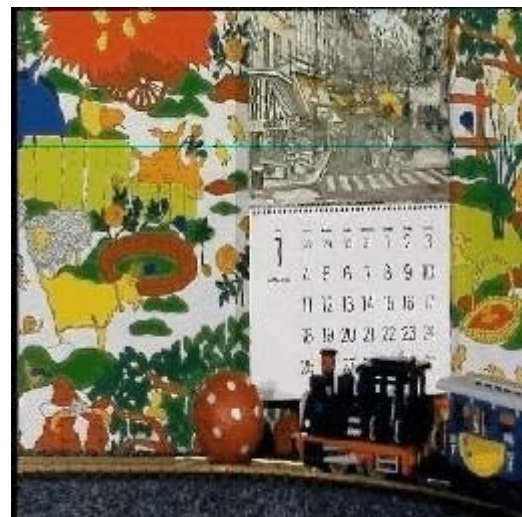
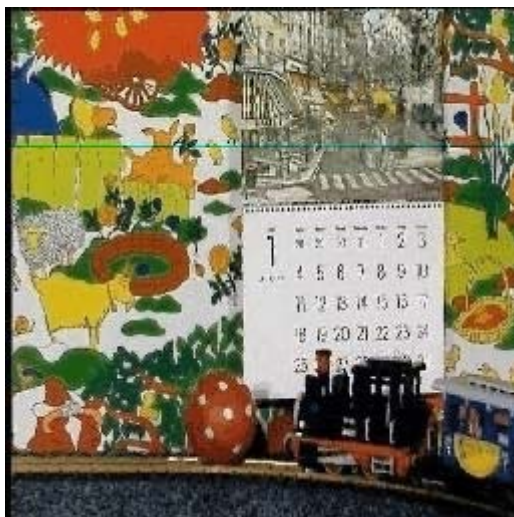
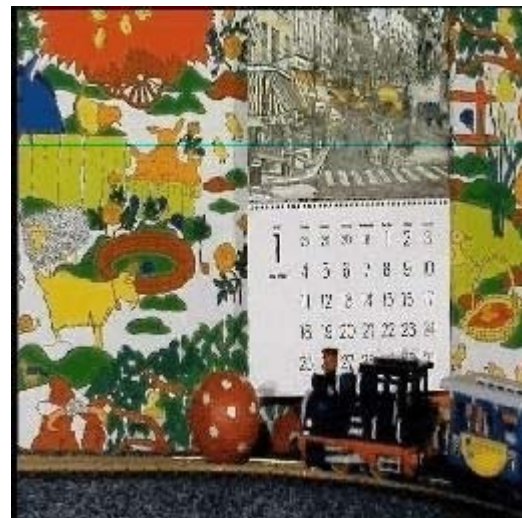
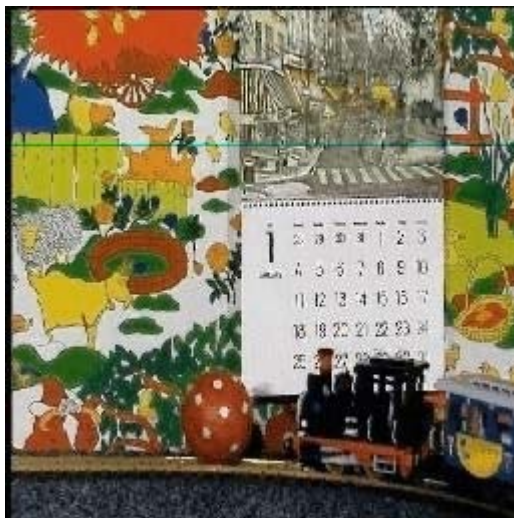
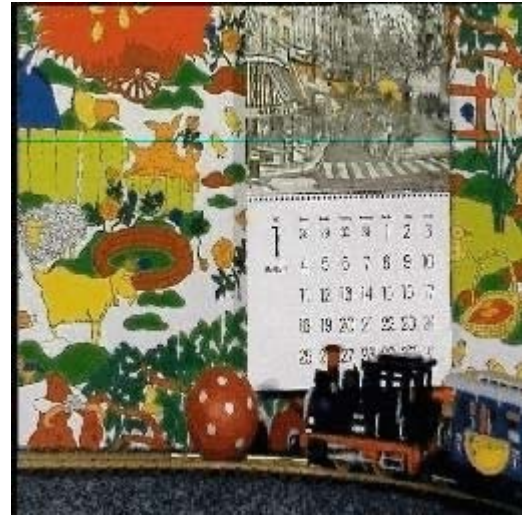
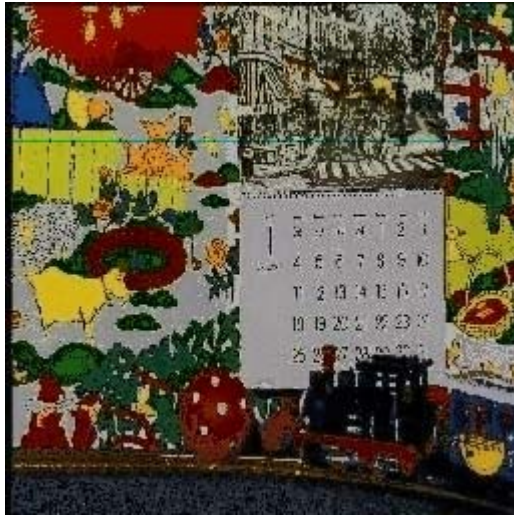
7. pixel_removed_video

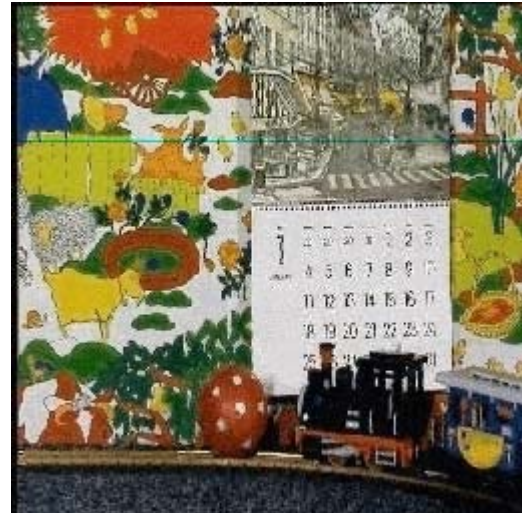




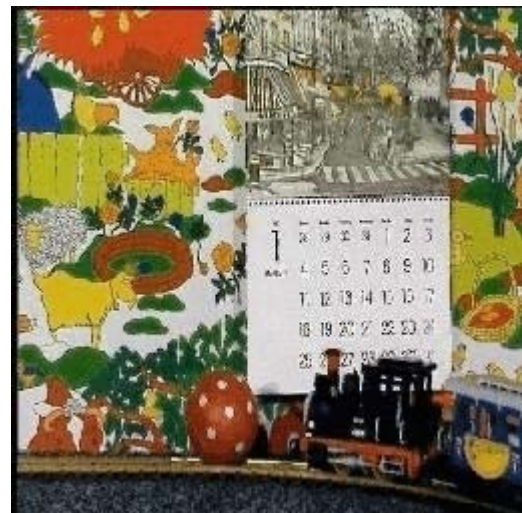
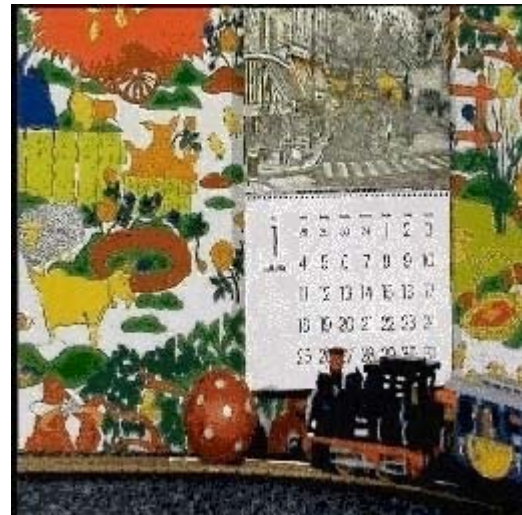
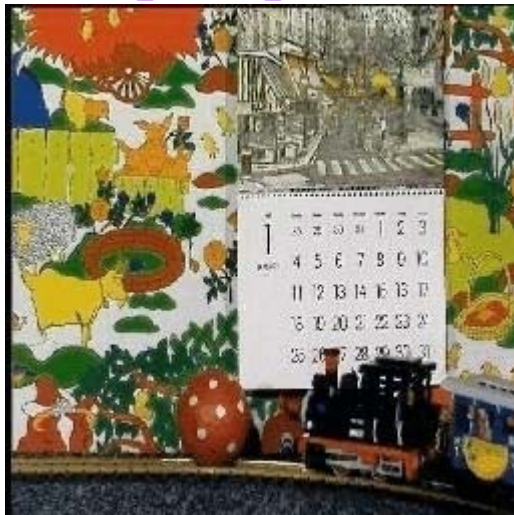
8. [line_removed_video](#)

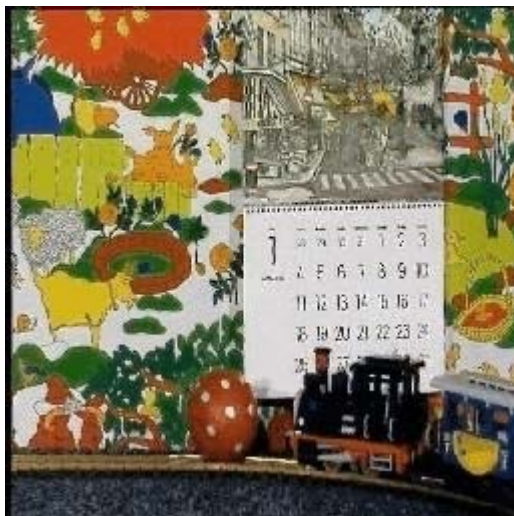
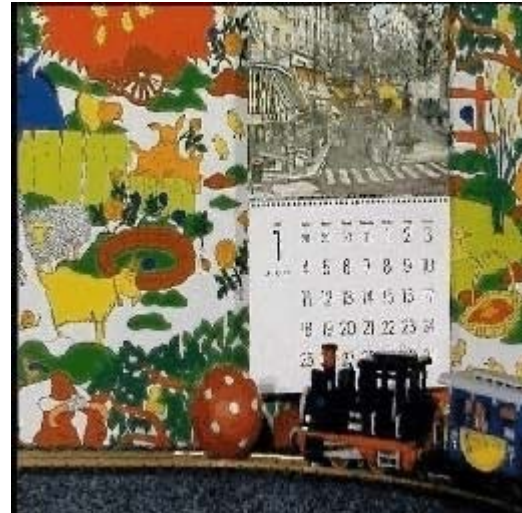
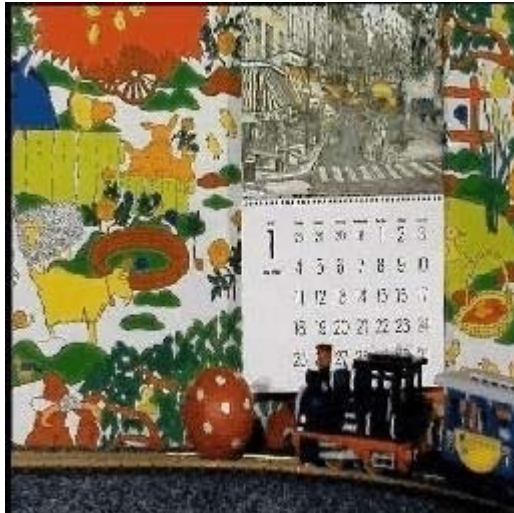






9. [frame_removed_video](#)





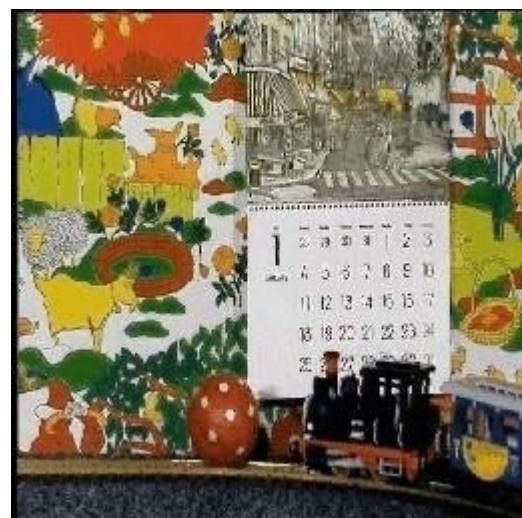
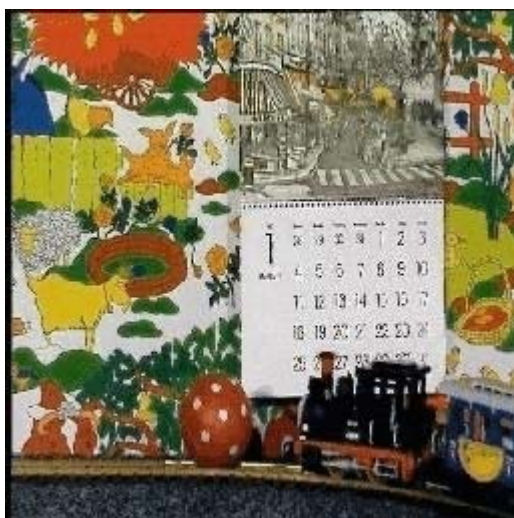
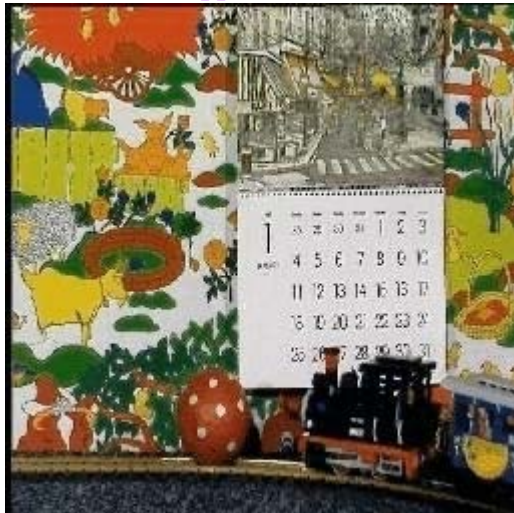
10. [frame_rotated_video](#)

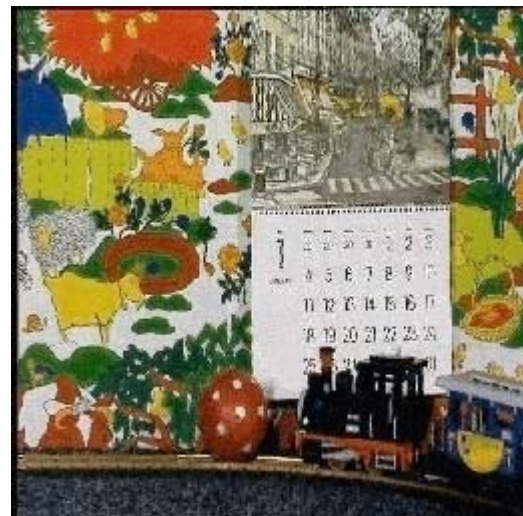
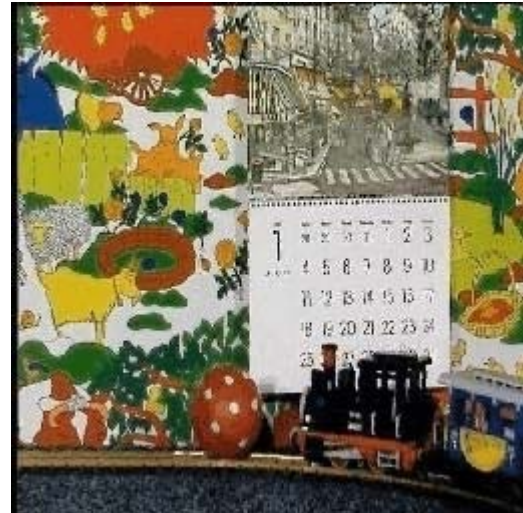
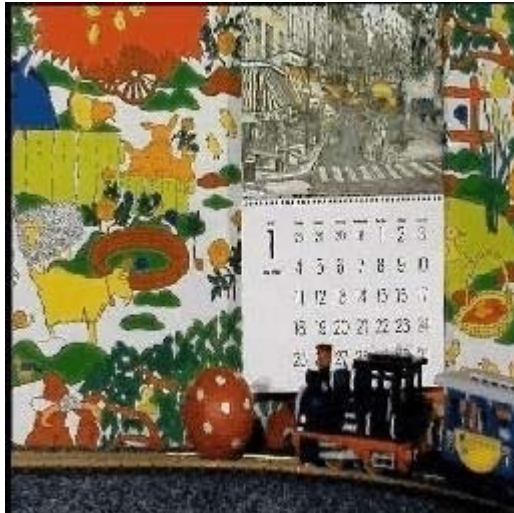




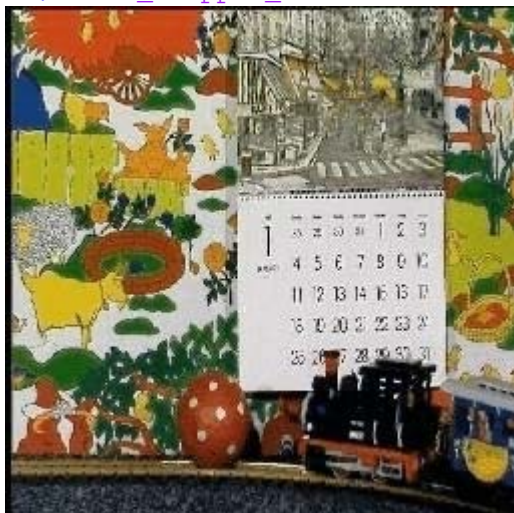


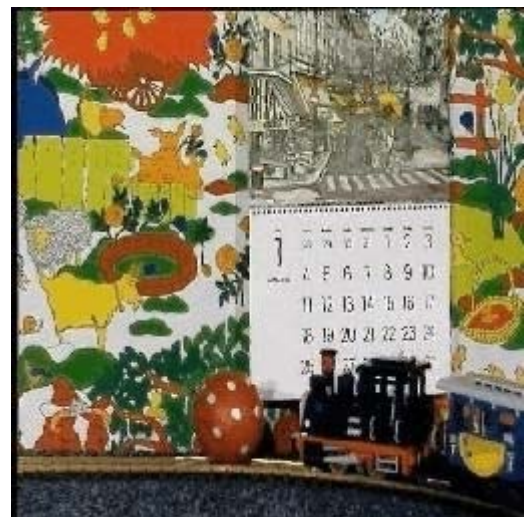
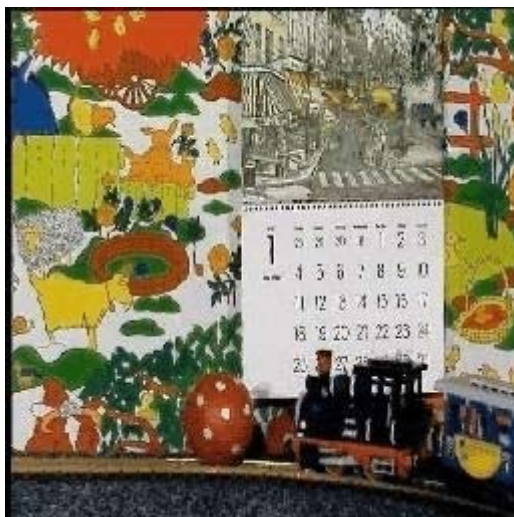
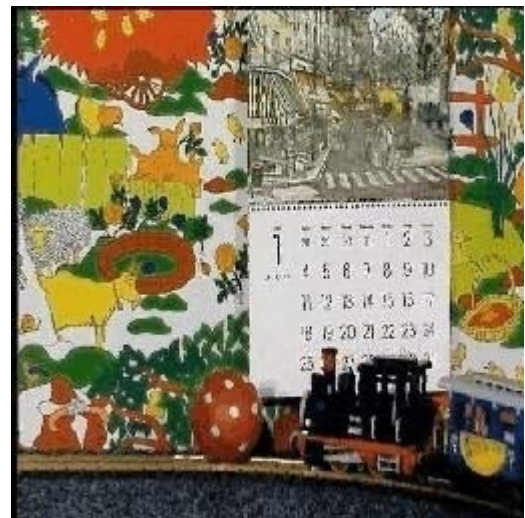
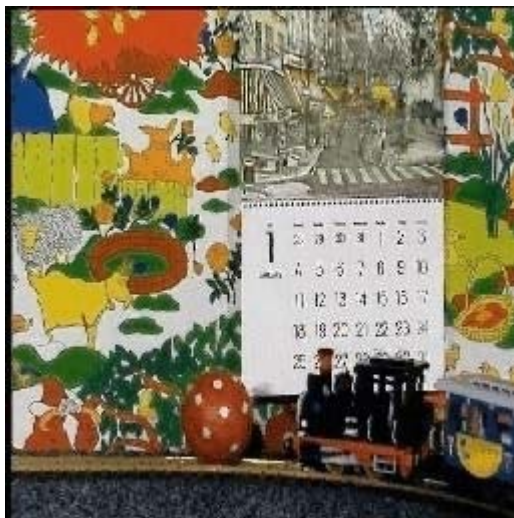
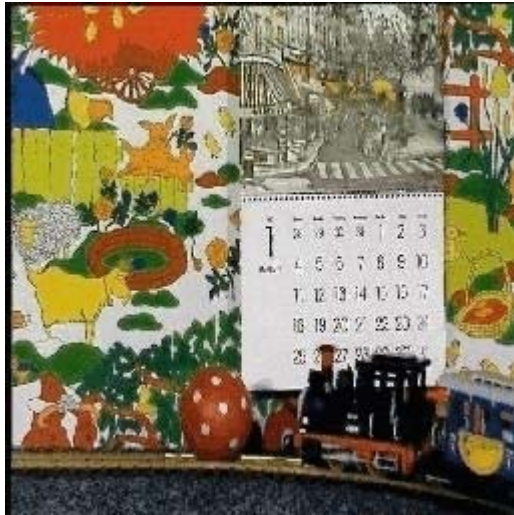
11. [frame_dropped_video](#)

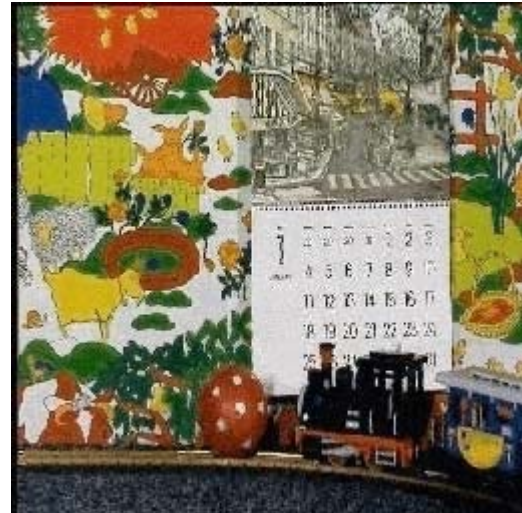




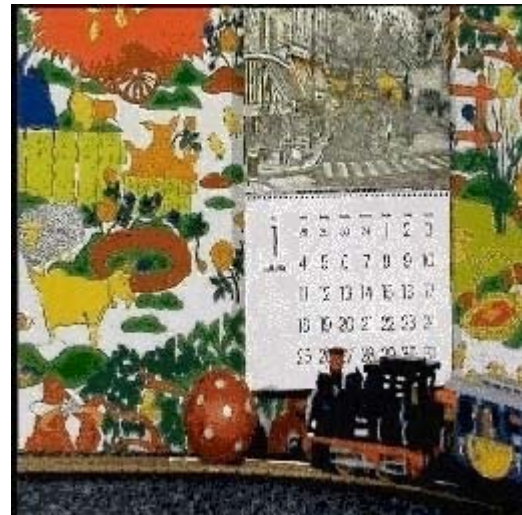
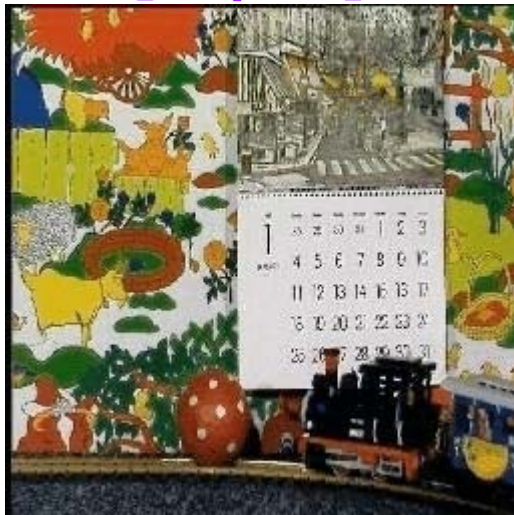
12. [frame_swapped_video](#)

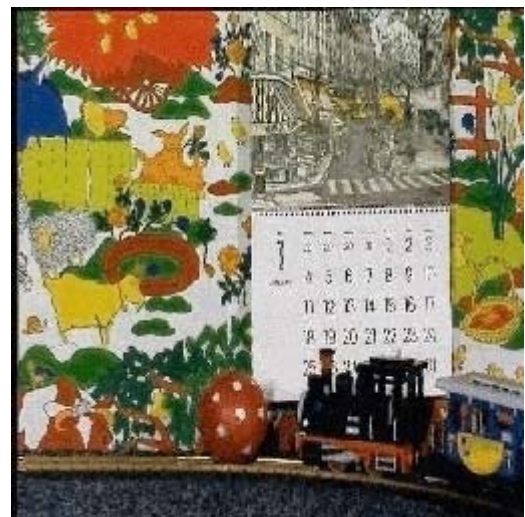
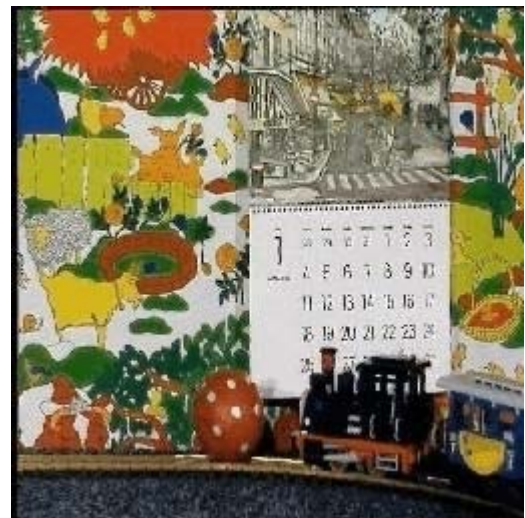




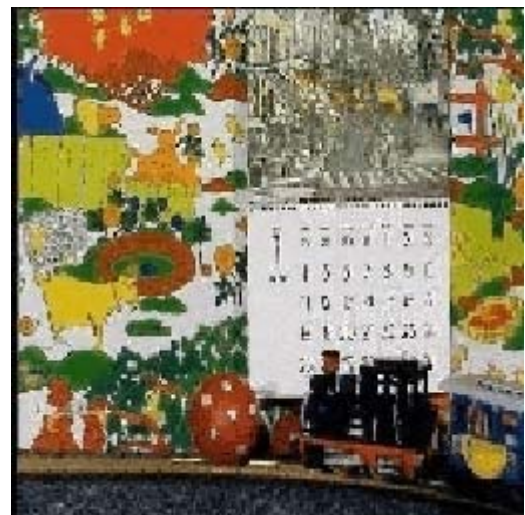
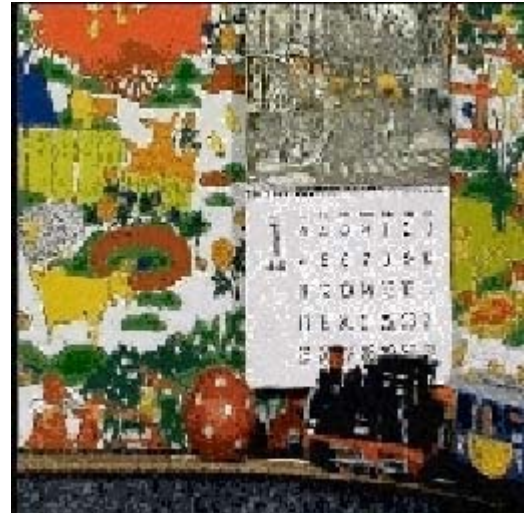


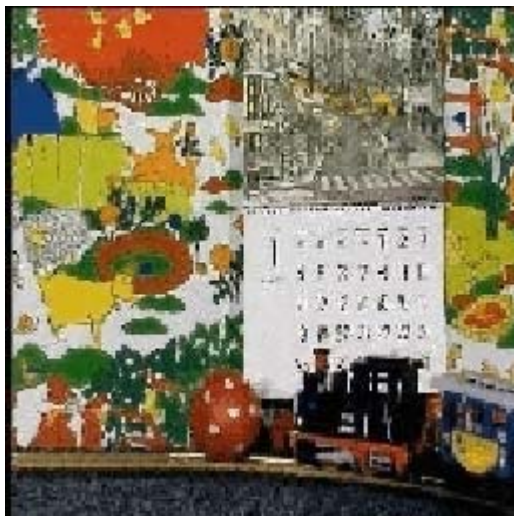
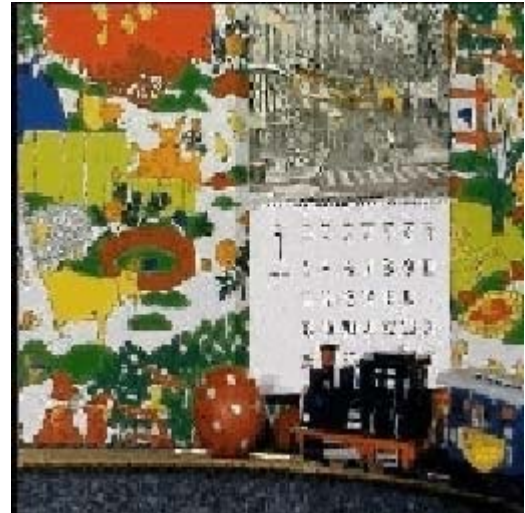
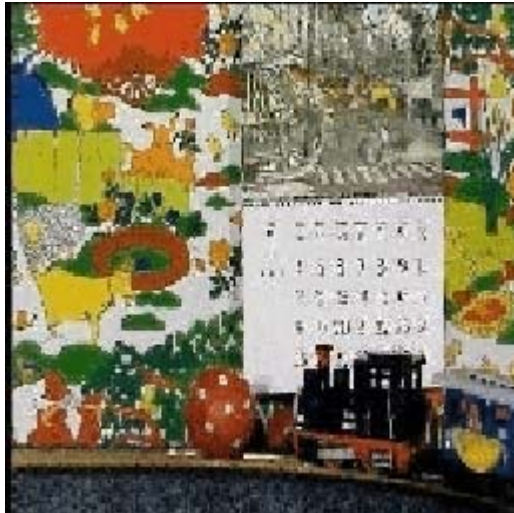
13. [frame_interpolated_video](#)





14. `frame_resized_video`





STAGE 3 : WATERMARK DETECTION

MODEL OF THE STAGE

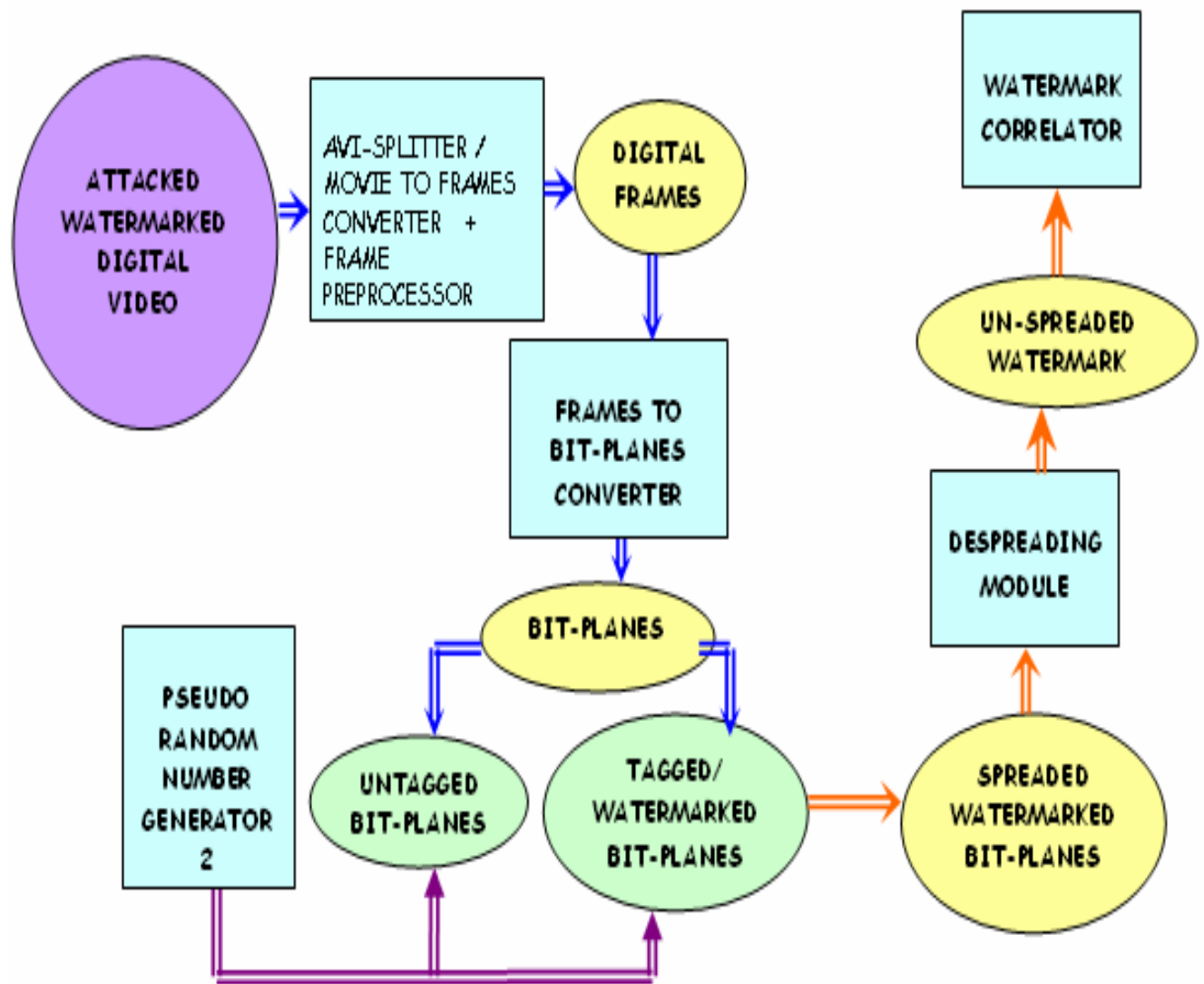


Figure 5.7 Model of the Stage III(Watermark Detection Stage)

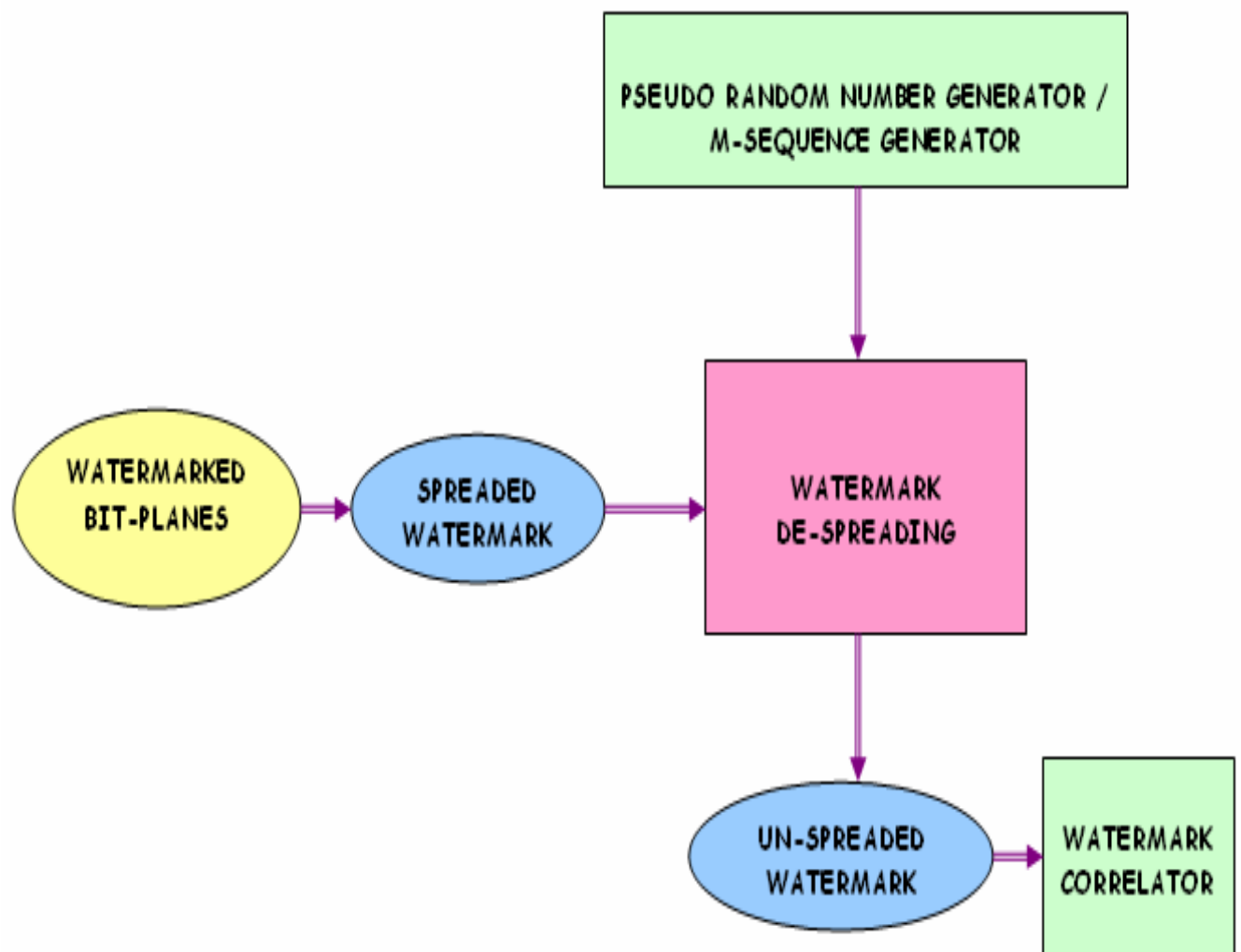
DE-SPREADING MODULE**VIDEO WATERMARKING : DE-SPREADING MODULE**

Figure 5.8 Model of the De-Spreading Module

WORKING OF THE STAGE

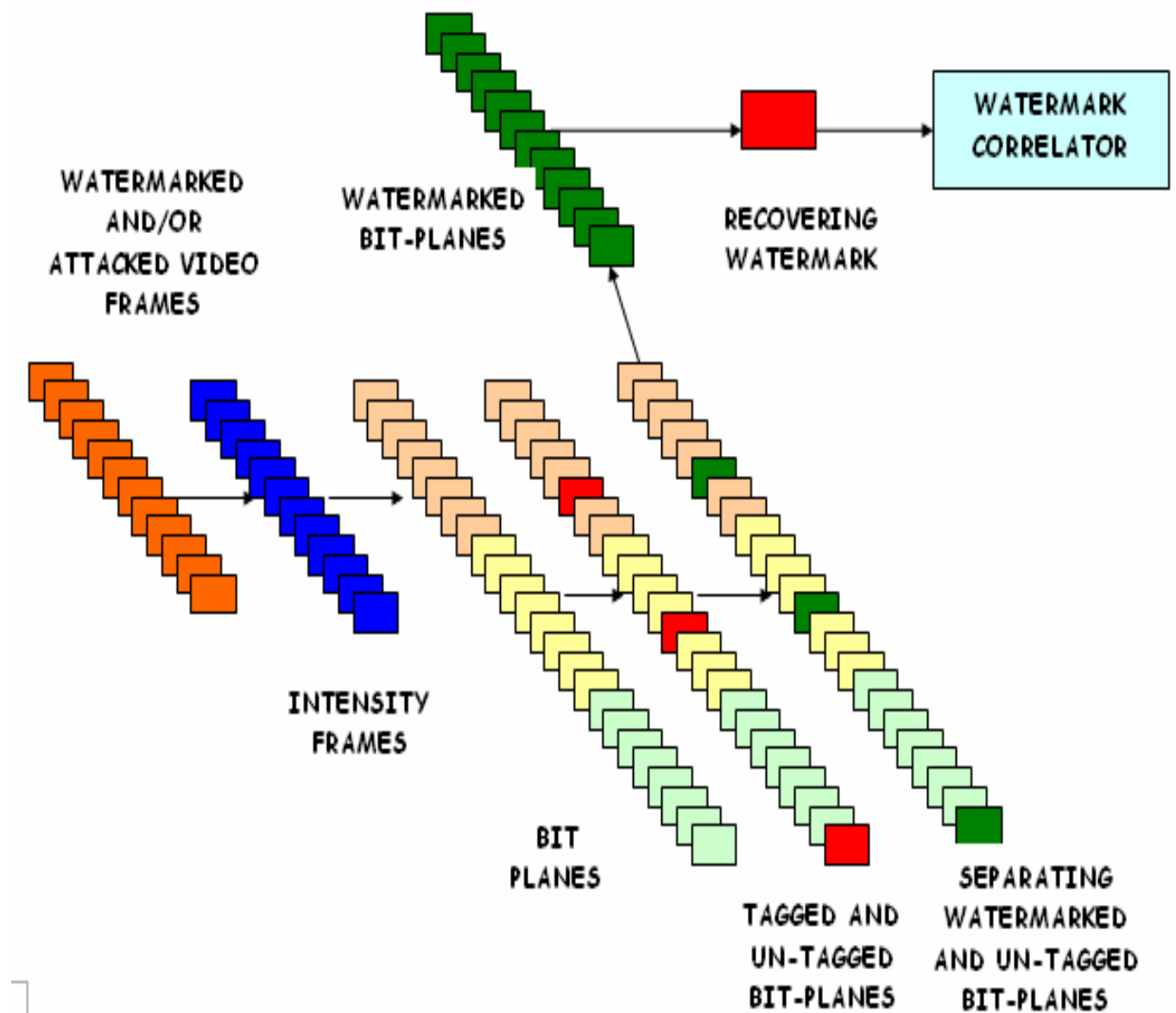


Figure 5.9 Working of the Stage III(Watermark Detection Stage)

MATLAB CODE SIMULATION RESULTS**DETECTED WATERMARKS
(WATERMARKING MSB PLANES)**

1. `watermarked_video`

A vertical watermark image. It consists of a dark, thick L-shaped border. Inside this border, the name 'MONICA GUPTA' is written in a white, bold, sans-serif font, arranged vertically from top to bottom.

2. compressed_video



3. `noisy_gaussian_video`



4. `noisy_salt_pepper_video`



5. averaged_filtered_video



6. median_filtered_video



7. wiener_filtered_video



8. pixel_removed_video



9. line_removed_video



10. `frame_removed_video`



11. `frame_rotated_video`



12. `frame_dropped_video`



13. frame_swapped_video



14. `frame_interpolated_video`



15. `frame_resized_video`



DETECTED WATERMARKS
(WATERMARKING MIDSUB PLANES)

1. `watermarked_video`



2. compressed_video



3. `noisy_gaussian_video`



4. `noisy_salt_pepper_video`



5. averaged_filtered_video



6. median_filtered_video



7. wiener_filtered_video



8. pixel_removed_video



9. `line_removed_video`



10. `frame_removed_video`



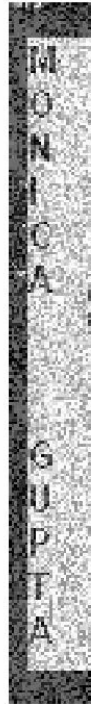
11. `frame_rotated_video`



12. `frame_dropped_video`



13. `frame_swapped_video`



14. `frame_interpolated_video`



15. frame_resized_video



DETECTED WATERMARKS

(WATERMARKING LSB PLANES)

1. `watermarked_video`



2. `compressed_video`



3. `noisy_gaussian_video`



4. `noisy_salt_pepper_video`



5. averaged_filtered_video



6. median_filtered_video



7. wiener_filtered_video



8. pixel_removed_video



9. `line_removed_video`



10. `frame_removed_video`



11. `frame_rotated_video`



12. `frame_dropped_video`



13. `frame_swapped_video`



14. `frame_interpolated_video`



15. `frame_resized_video`



6. CONCLUSION

Summary--:

This section is concerned with critically evaluating the watermarking method employed. Also experiments were run on the code and the results graphed. There are many important factors to consider in a project of this kind, the type of the watermark, the plane chosen for Watermark Insertion and so forth. All appropriate graphs are drawn from figures generated by the code itself and graphed directly in Microsoft Word.

There are several trade offs in the area of Digital Video Watermarking. Improving certain aspects nearly always ensures that certain other aspects deteriorate. The most important are discussed below, since they had the largest bearing on the progress of this project.

The first task is to check for the visibility of the watermark. As can be seen from the watermarked frames and the WPSNR values which are 11.8770499(IN DB), 20.4629089 (IN DB) and 25.5178578 (IN DB) respectively for MSB region, MID-SB region and LSB region that the watermark is more visible in case when MSB region is chosen for watermarking. The watermark becomes less visible as we move from MSB region to MID-SB region and then from MID-SB region to LSB region.

Now comes the issue of Watermark robustness. It was determined that the highest 4 bit planes, that is MSB region, constitute safe places to hold the watermark. It is verified that in this case the extracted watermark planes correlate much higher with the original watermark planes than image planes. Robustness of the watermark to noise is of interest. Noise may be added to Video to make the watermark undetectable. This approach of course can be self defeating since Video quality degrades as well. It is shown that the Video quality gives out long before the embedded Watermark.

EXPERIMENTAL RESULTS--:

I have used a 1 seconds long Video with frame size of 256x256 pixels for a total of 10 frames.

For the placement of the Watermark in the Video corresponding to the **LSB region**(bit-planes 1,2,3,4) one of the 4 lower bitplanes is pseudorandomly chosen. The 10 bit-planes chosen for 10 frames are { 1 4 2 3 1 2 2 2 1 4 } resp, where 1 corresponds to the LSB plane. The

watermarked and original video remains virtually indistinguishable even when viewed on a monitor.

Now , What we are talking about is the impact of frame drops, random or regular, which may arise either intentionally or otherwise. To check for this phenomenon, we tested watermark recovery on the above footage. Random frame drops pose a more serious challenge. This process is defined by frame removals at random intervals and random frequency. There is an interaction between the time separating frame drops.

For the MID-SB region bitplanes chosen are {3 6 4 5 3 6 4 5 3 4}resp. For the MSB-region bitplanes selected are {5 7 6 8 8 6 7 5 5 7 }resp.

In this work we have shown that results from work in CDMA can be brought to bear on Video Watermarking if similarities and differences are properly distinguished. The rich and multidimensional content of video opens up exciting extensions of the traditional signal-based work in CDMA. By the same token, the varied and complex nature of attacks on watermark removal goes beyond the known problems that conventional CDMA signals have to cope with. However, the simplicity of watermark embedding and retrieval that is done at bitplane level makes CDMA watermarking attractive in many multimedia applications. This includes large scale watermarking of multimedia titles by using a family of near orthogonal PN sequences.

TAB 1.1 COMPARISON TABLE (WATERMARKING MSB PLANES)

SR. NO.	TYPE OF WATERMARKED VIDEO	WPSNR VALUE (IN DB)	CORRELATION VALUE (IN DB)
1.	UNATTACKED WATERMARKED VIDEO	74031105.	42.76027
2.	COMPRESSED WATERMARKED VIDEO	103.97940	42.62730
3.	NOISY(GAUSSIAN) WATERMARKED VIDEO	11.76866	42.33058
4.	NOISY(SALT & PEPPER) WATERMARKED VIDEO	105.74031	42.75933
5.	AVERAGE FILTERED WATERMARKED VIDEO	7.10603	42.09642
6.	MEDIAN FILTERED WATERMARKED VIDEO	8.69034	42.40184
7.	WIENER FILTERED WATERMARKED VIDEO	11.58644	42.58419
8.	PIXEL REMOVED WATERMARKED VIDEO	105.74031	42.75986
9.	LINE REMOVED WATERMARKED VIDEO	14.00388	42.75753
10.	FRAME REMOVED WATERMARKED VIDEO	100.96910	42.30611
11.	FRAME ROTATED WATERMARKED VIDEO	5.26089	41.46110
12.	FRAME DROPPED WATERMARKED VIDEO	7.83133	41.98779
13.	FRAME SWAPPED WATERMARKED VIDEO	100.96910	42.65890
14.	FRAME INTERPOLATED WATERMARKED VIDEO	100.96910	42.68041
15.	FRAME RESIZED WATERMARKED VIDEO	9.68434	42.49543

TAB 1.2 COMPARISON TABLE (WATERMARKING MDSB PLANES)

SR. NO.	TYPE OF WATERMARKED VIDEO	WPSNR VALUE (IN DB)	CORRELATION VALUE (IN DB)
1.	UNATTACKED WATERMARKED VIDEO	13.52162	42.75818
2.	COMPRESSED WATERMARKED VIDEO	9.32553	42.53660
3.	NOISY(GAUSSIAN) WATERMARKED VIDEO	6.76572	42.11660
4.	NOISY(SALT & PEPPER) WATERMARKED VIDEO	13.32512	42.75754
5.	AVERAGE FILTERED WATERMARKED VIDEO	6.13199	42.06379
6.	MEDIAN FILTERED WATERMARKED VIDEO	7.77884	42.36815
7.	WIENER FILTERED WATERMARKED VIDEO	8.90655	42.46240
8.	PIXEL REMOVED WATERMARKED VIDEO	13.42684	42.75802
9.	LINE REMOVED WATERMARKED VIDEO	13.19362	42.75593
10.	FRAME REMOVED WATERMARKED VIDEO	10.71090	41.97366
11.	FRAME ROTATED WATERMARKED VIDEO	5.21541	41.47886
12.	FRAME DROPPED WATERMARKED VIDEO	7.20314	41.96130
13.	FRAME SWAPPED WATERMARKED VIDEO	11.08909	42.65455
14.	FRAME INTERPOLATED WATERMARKED VIDEO	12.26828	42.67096
15.	FRAME RESIZED WATERMARKED VIDEO	9.44666	42.50569

TAB 1.3 COMPARISON TABLE (WATERMARKING LSB PLANES)

SR. NO.	TYPE OF WATERMARKED VIDEO	WPSNR VALUE (IN DB)	CORRELATION VALUE (IN DB)
1.	UNATTACKED WATERMARKED VIDEO	10.37356	42.60753
2.	COMPRESSED WATERMARKED VIDEO	5.79322	41.97258
3.	NOISY(GAUSSIAN) WATERMARKED VIDEO	5.72204	41.99257
4.	NOISY(SALT & PEPPER) WATERMARKED VIDEO	10.11601	42.58388
5.	AVERAGE FILTERED WATERMARKED VIDEO	5.74295	41.96905
6.	MEDIAN FILTERED WATERMARKED VIDEO	6.49070	42.10196
7.	WIENER FILTERED WATERMARKED VIDEO	5.99368	41.97487
8.	PIXEL REMOVED WATERMARKED VIDEO	10.29709	42.59878
9.	LINE REMOVED WATERMARKED VIDEO	10.21187	42.59620
10.	FRAME REMOVED WATERMARKED VIDEO	9.39642	42.36540
11.	FRAME ROTATED WATERMARKED VIDEO	5.20732	41.48609
12.	FRAME DROPPED WATERMARKED VIDEO	5.87860	42.05949
13.	FRAME SWAPPED WATERMARKED VIDEO	8.49667	42.60600
14.	FRAME INTERPOLATED WATERMARKED VIDEO	9.03793	42.50943
15.	FRAME RESIZED WATERMARKED VIDEO	7.93948	42.36797

RANDOM WATERMAR 2



RANDOM WATERMAR 3



RANDOM WATERMAR 4



RANDOM WATERMAR 5

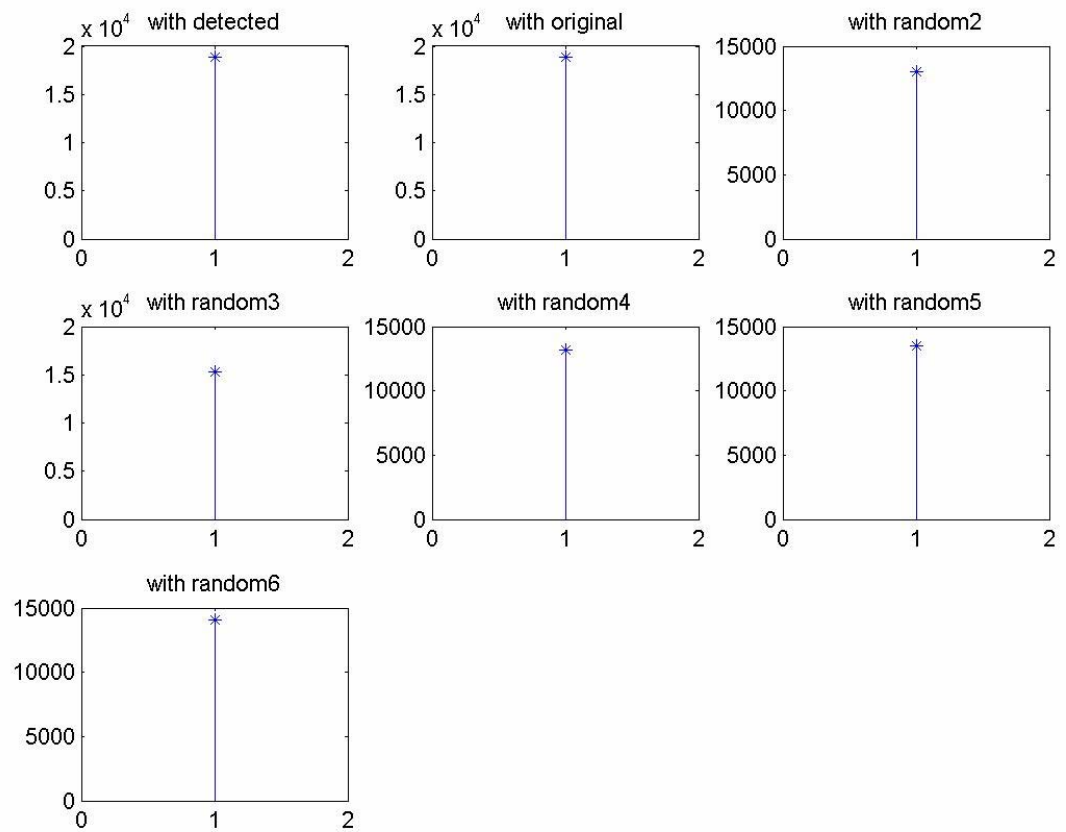


RANDOM WATERMAR 6

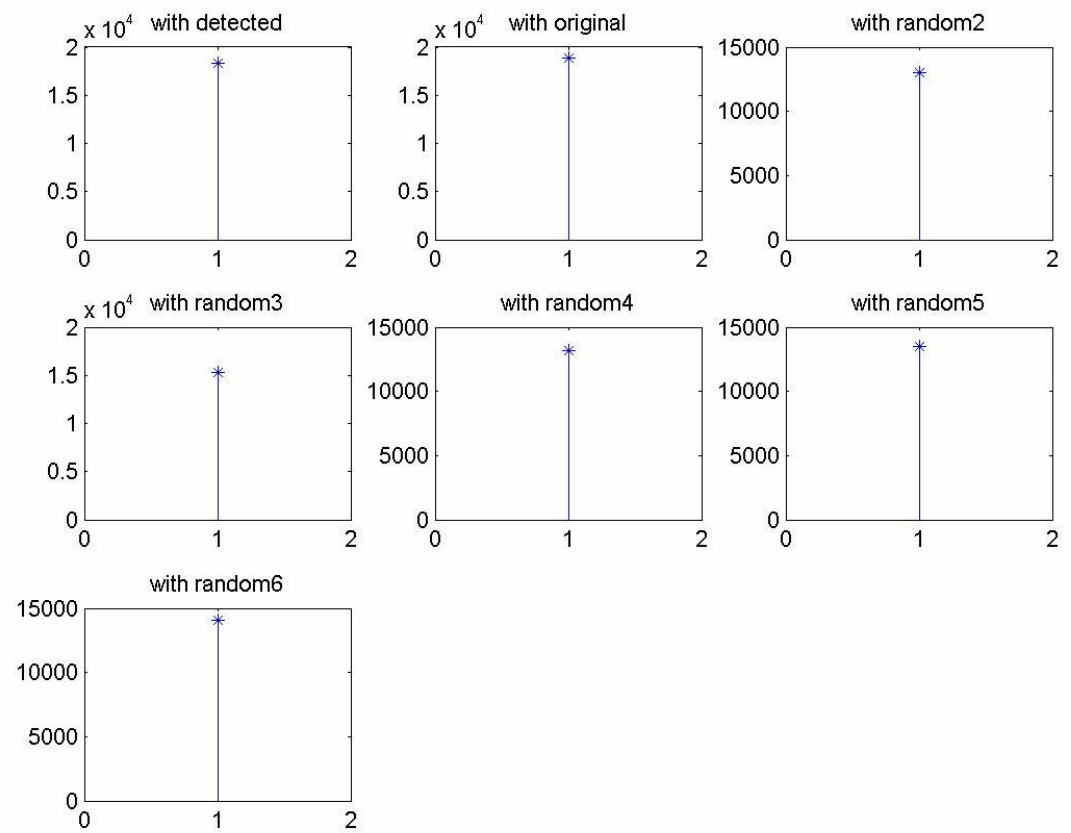


GRAPHICAL DISPLAY OF CORRELATION VALUES (WATERMARKING MSB PLANES)

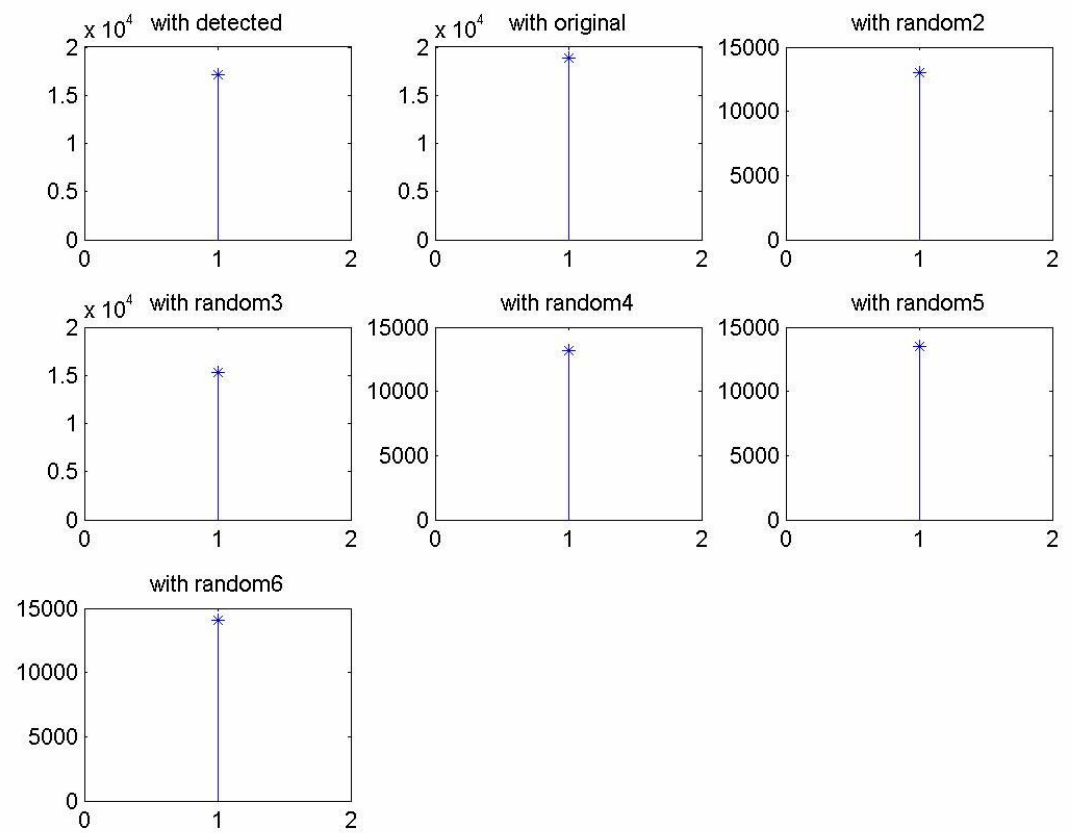
1. watermarked_video



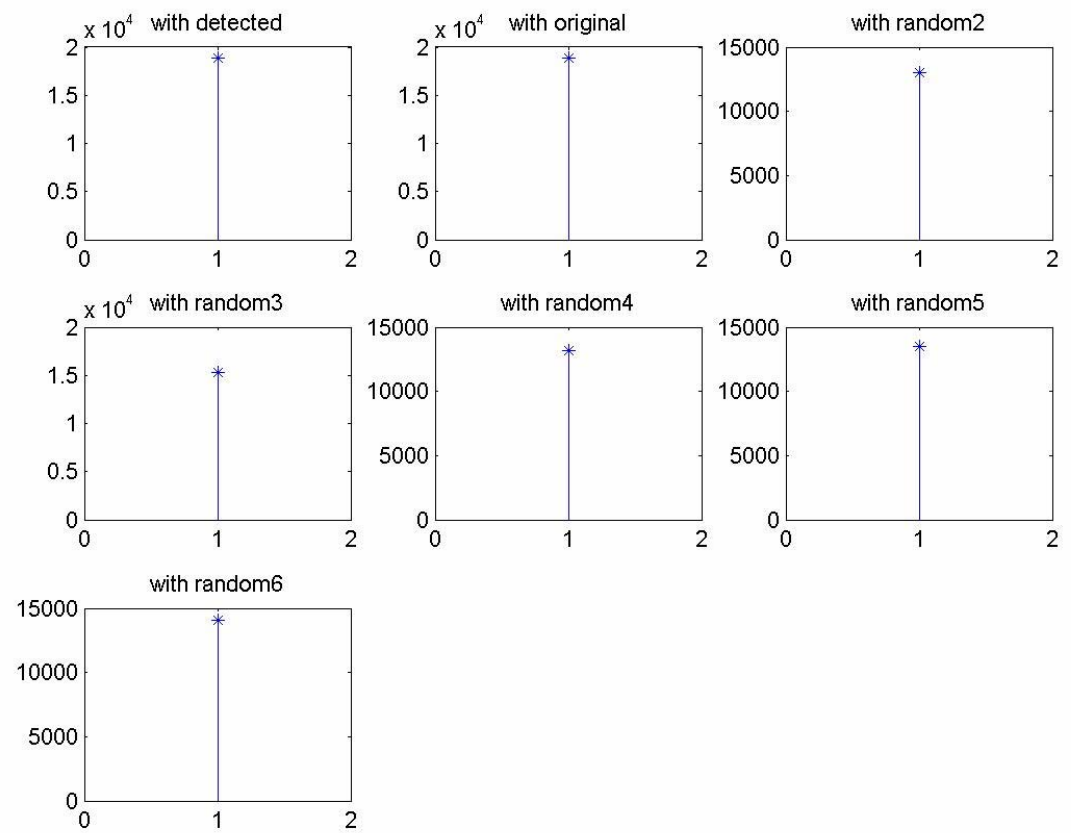
2. compressed_video



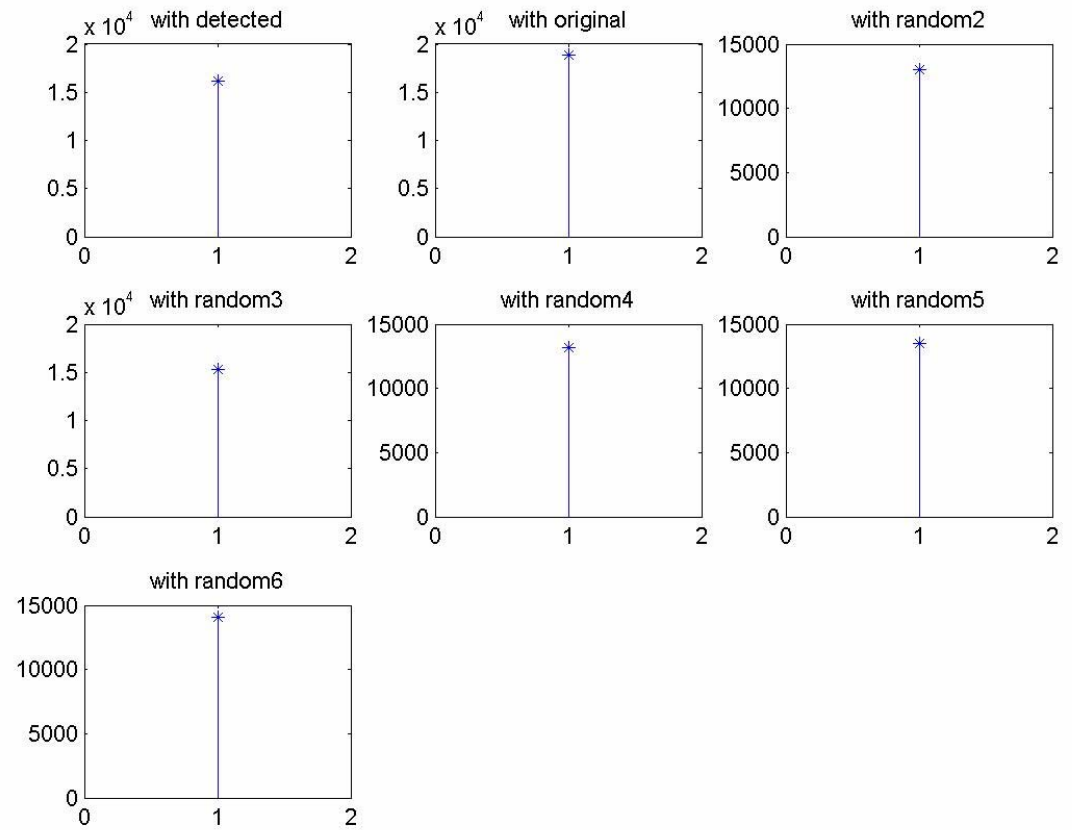
3. noisy_gaussian_video



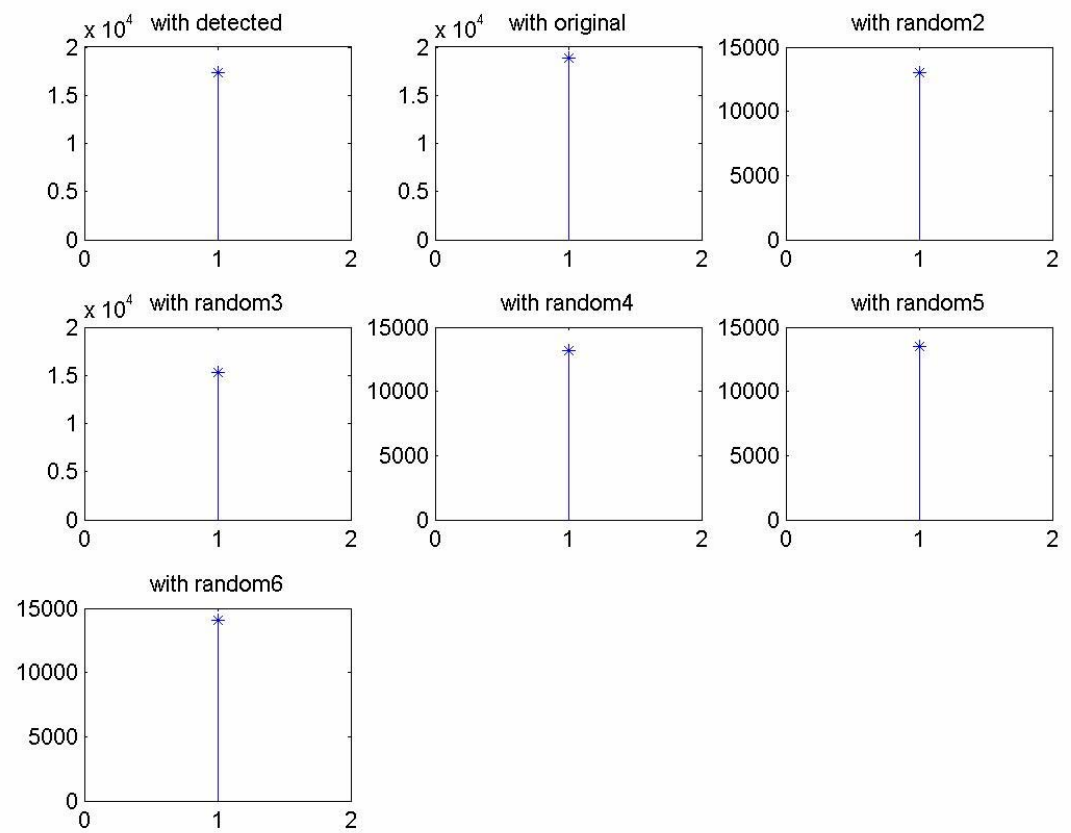
4. noisy_salt_pepper_video



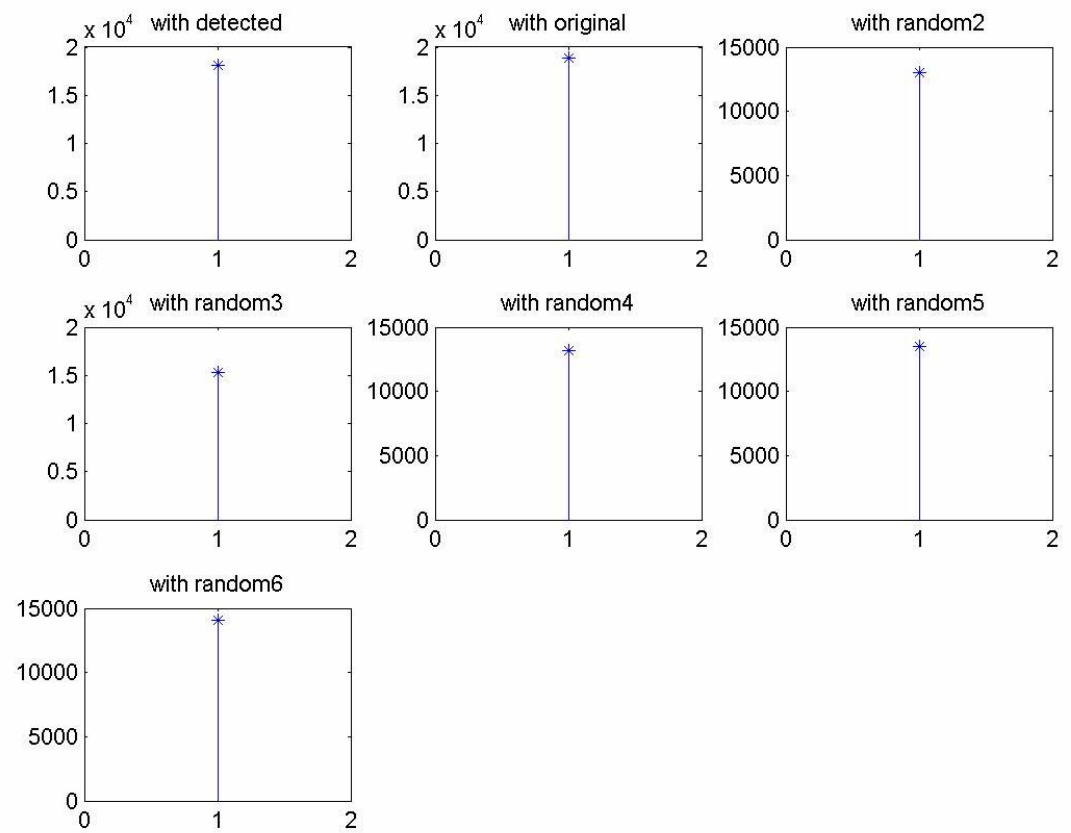
5. averaged_filtered_video



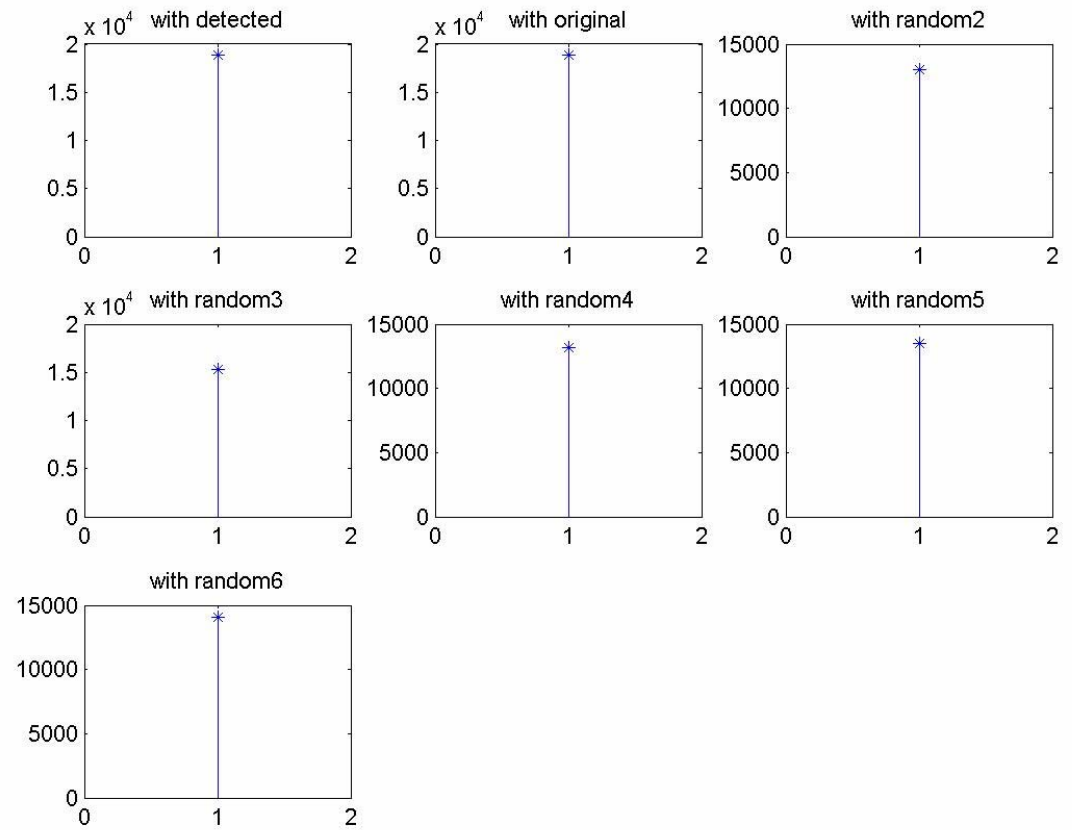
6. median_filtered_video



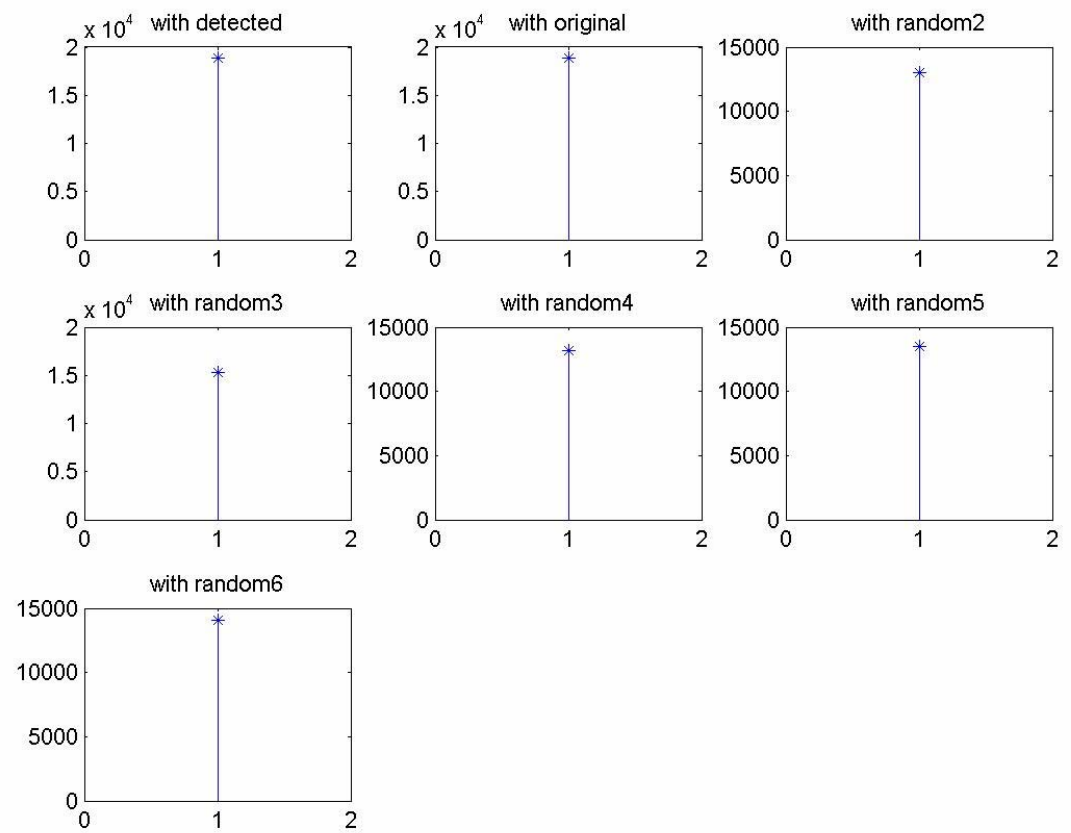
7. wiener_filtered_video



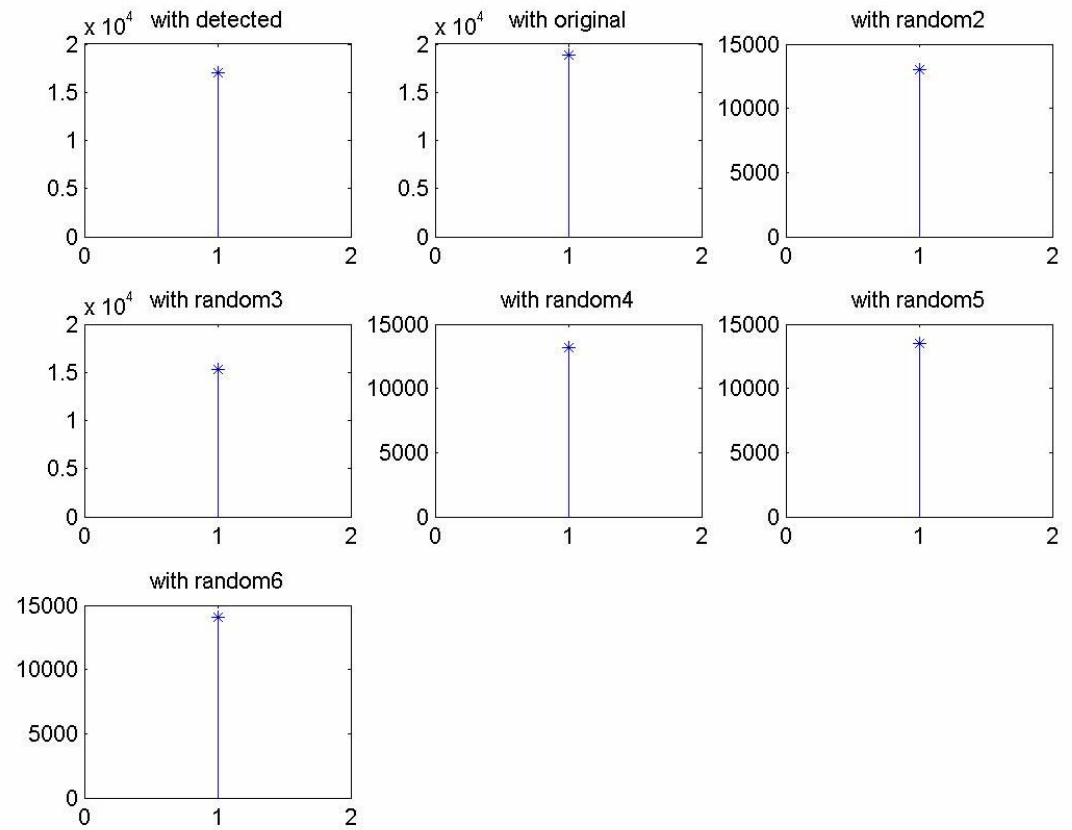
8. pixel_removed_video



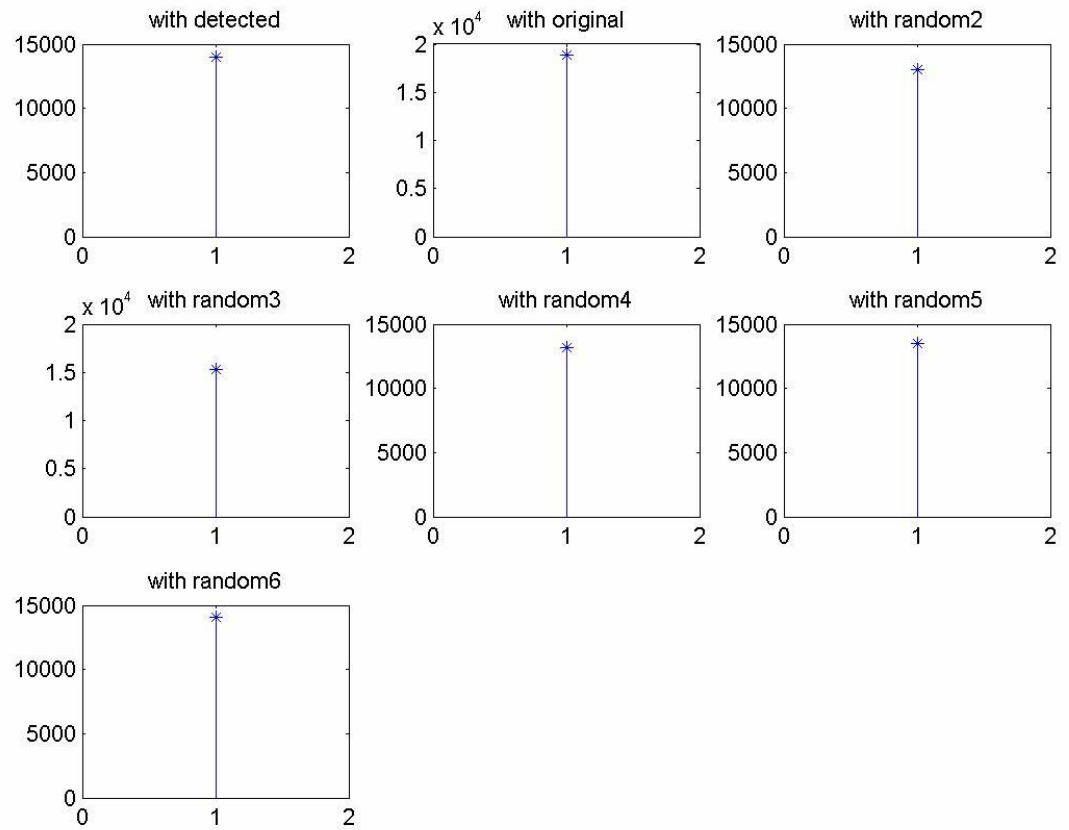
9. line_removed_video



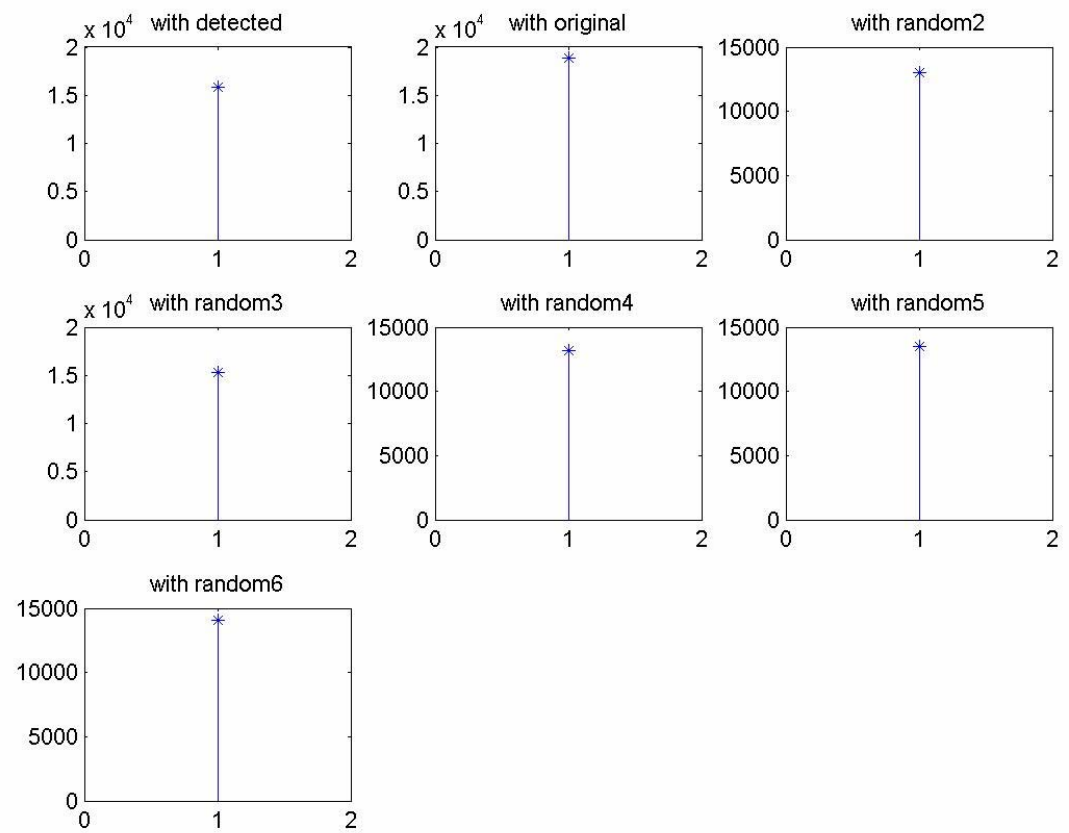
10. frame_removed_video



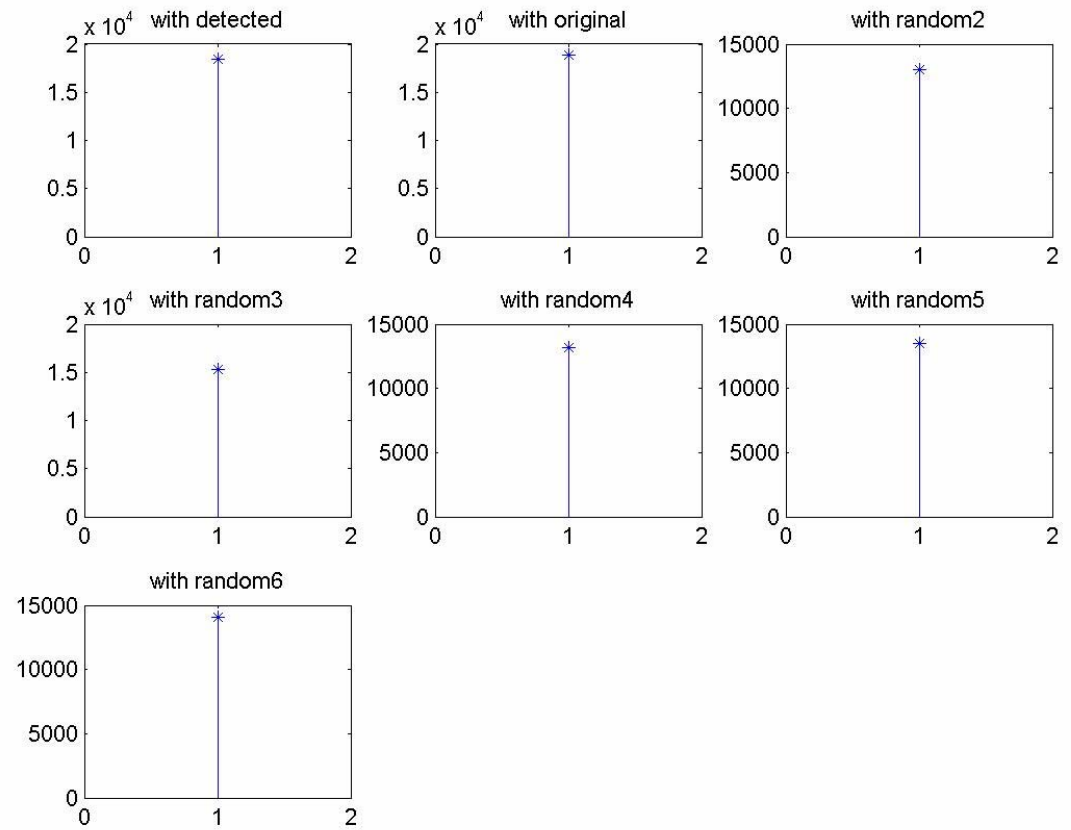
11. frame_rotated_video



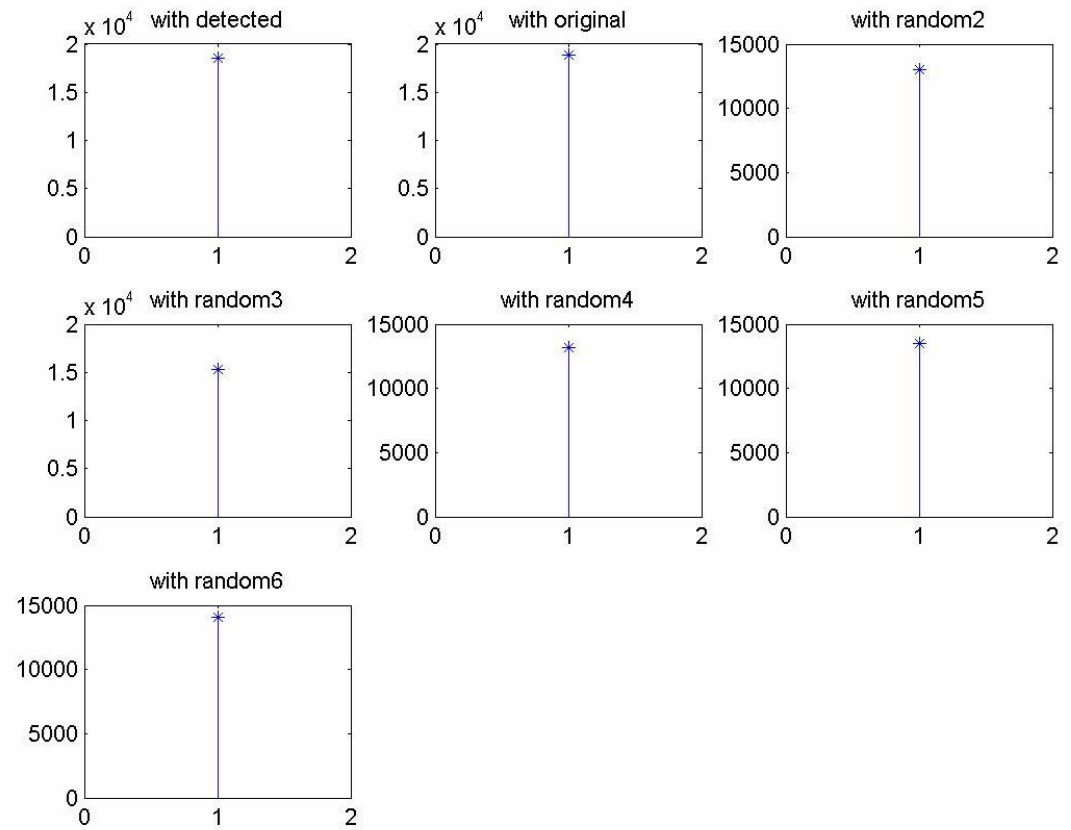
12. frame_dropped_video



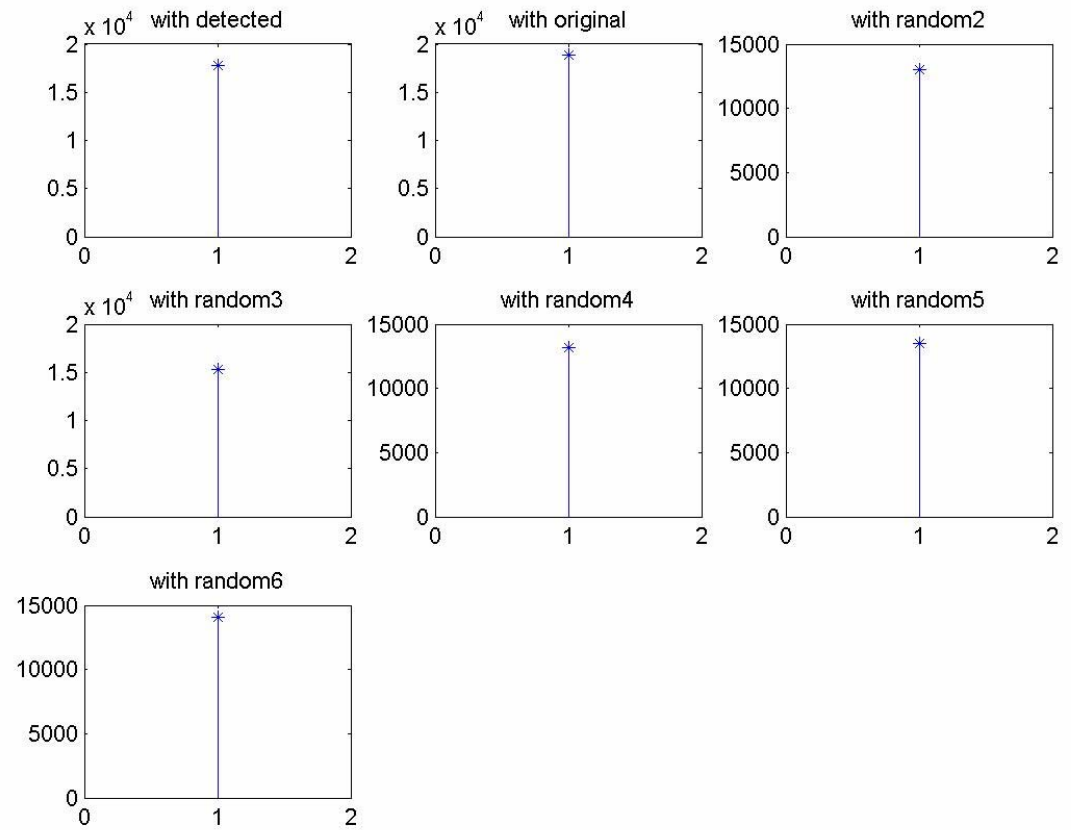
13. frame_swapped_video



14. frame_interpolated_video

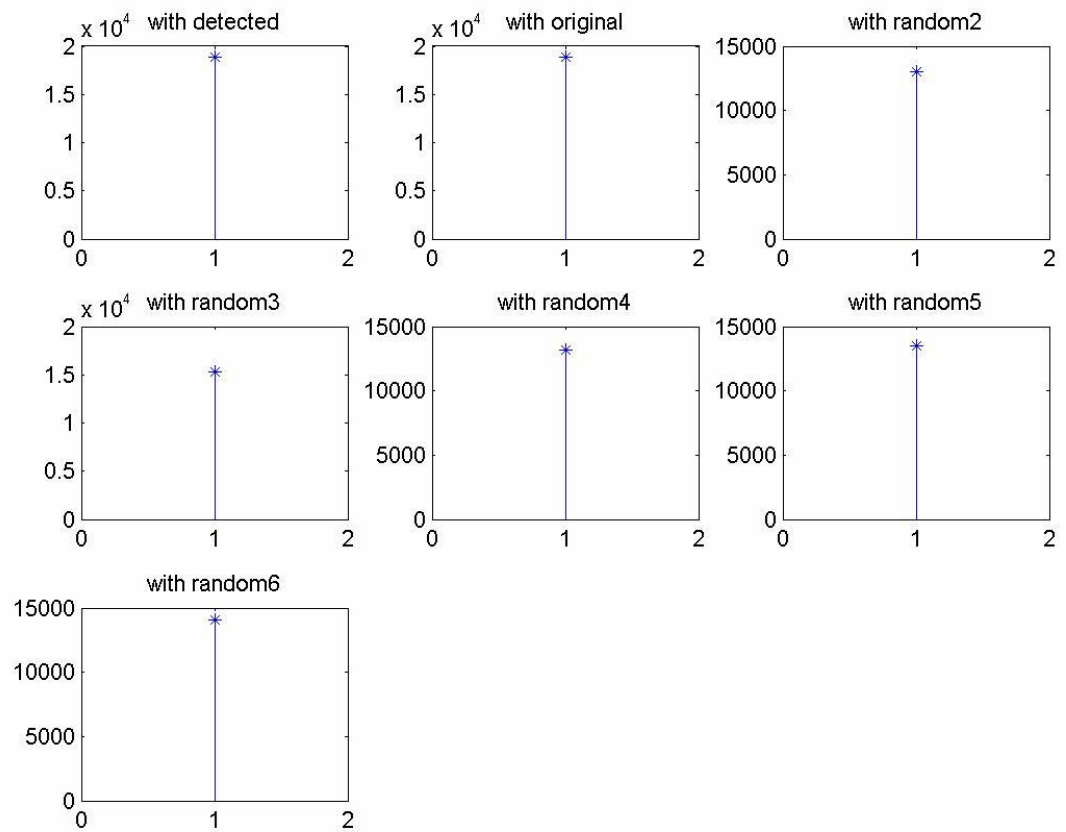


15. frame_resized_video

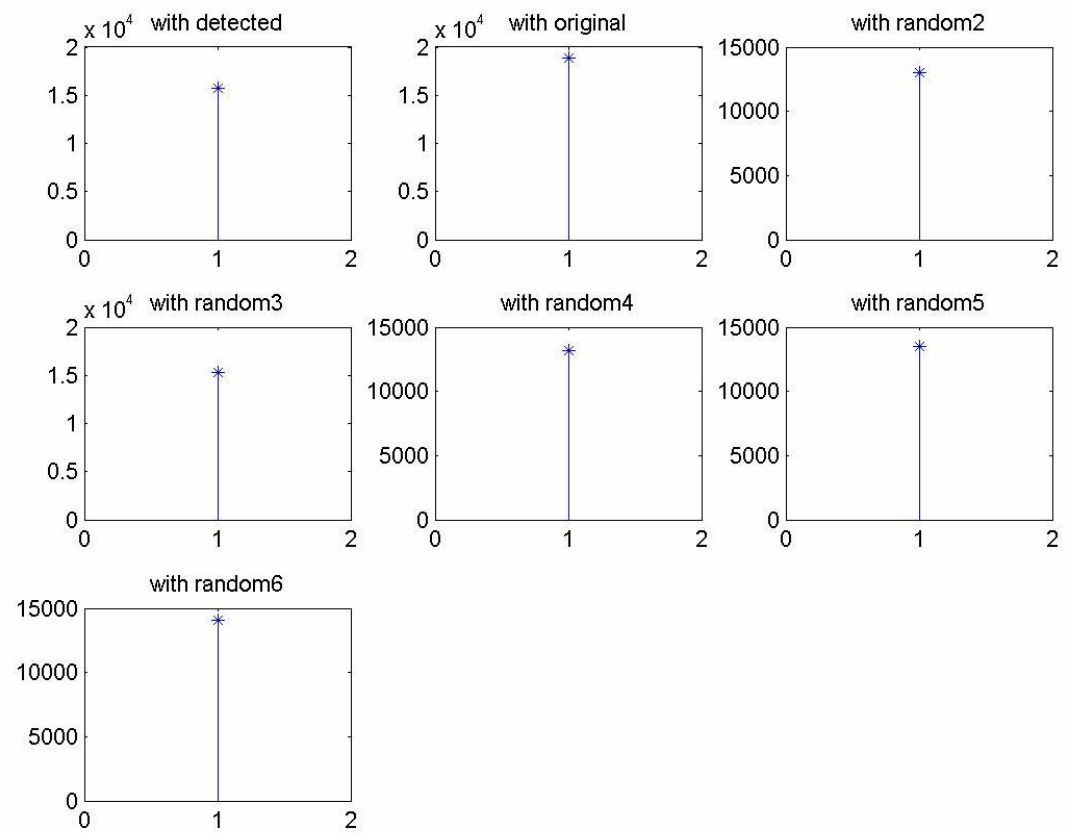


GRAPHICAL DISPLAY OF CORRELATION VALUES (WATERMARKING MID-SB PLANES)

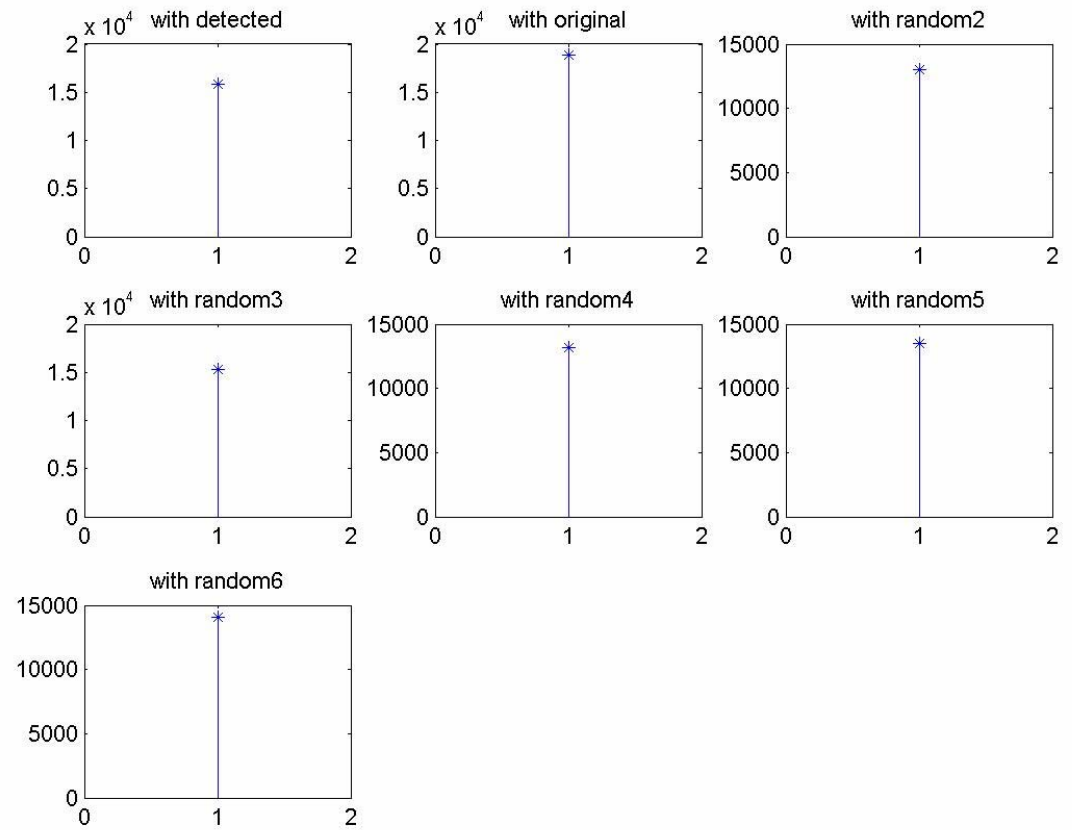
1. watermarked_video



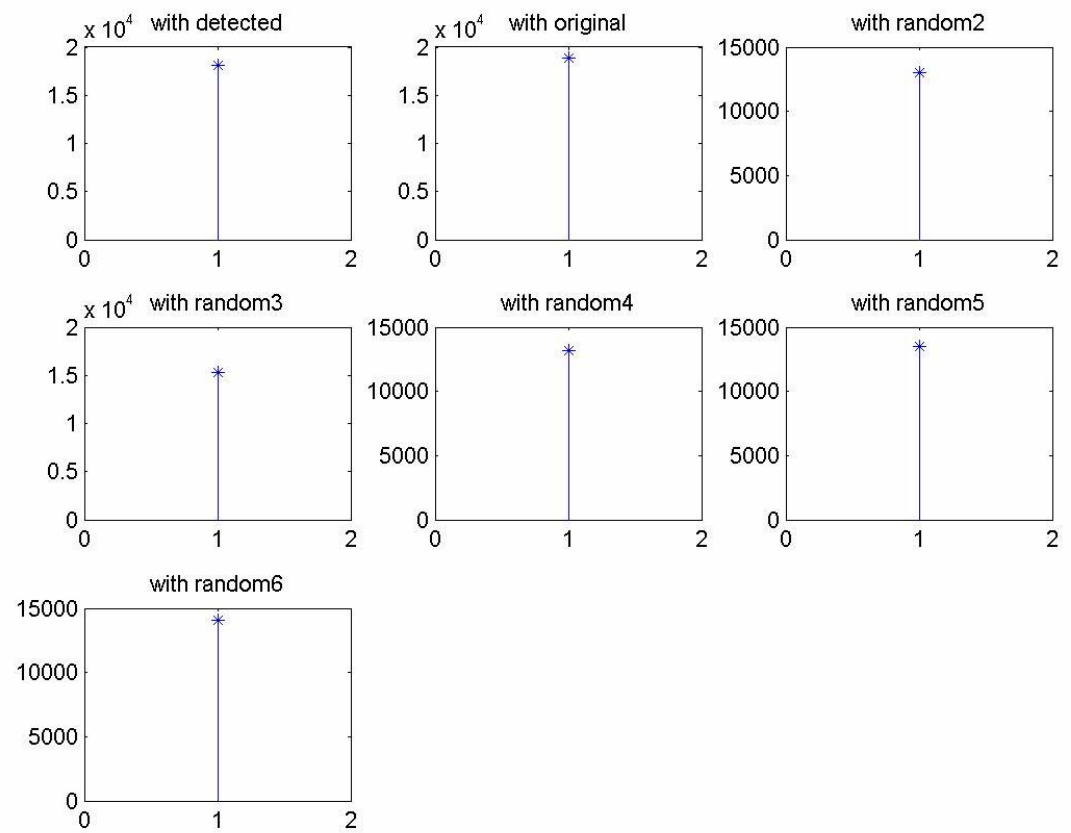
2. compressed_video



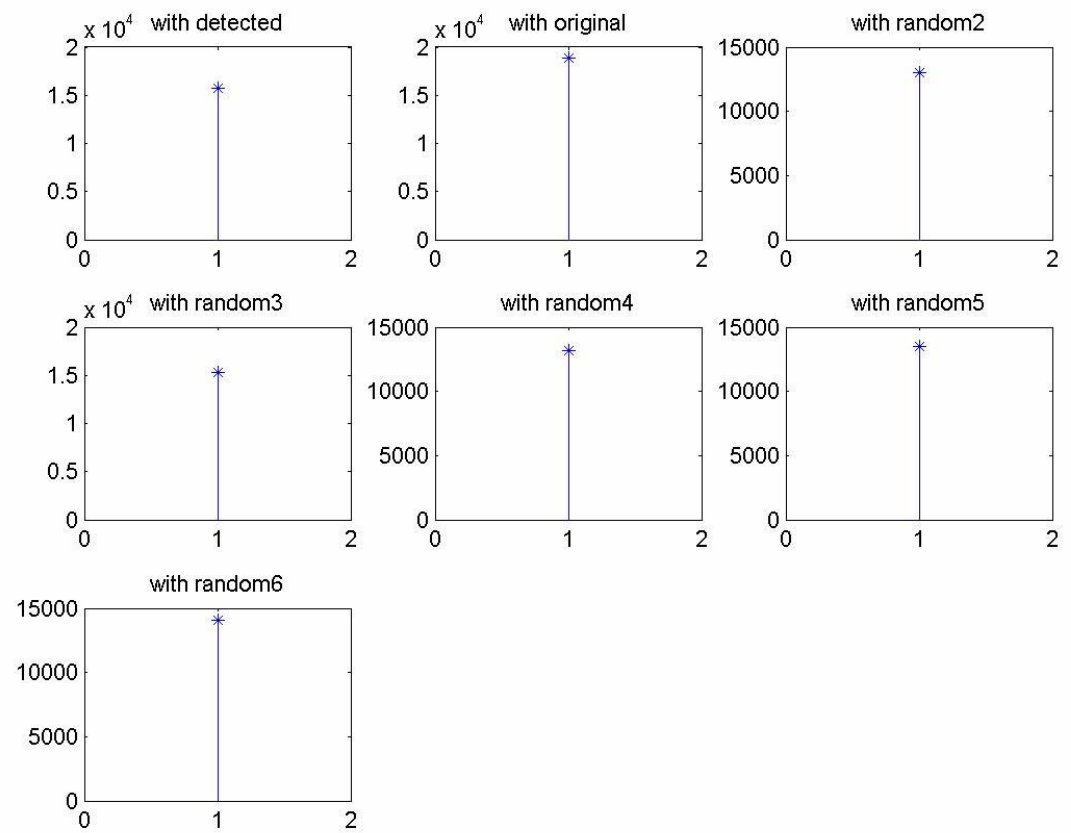
3. noisy_gaussian_video



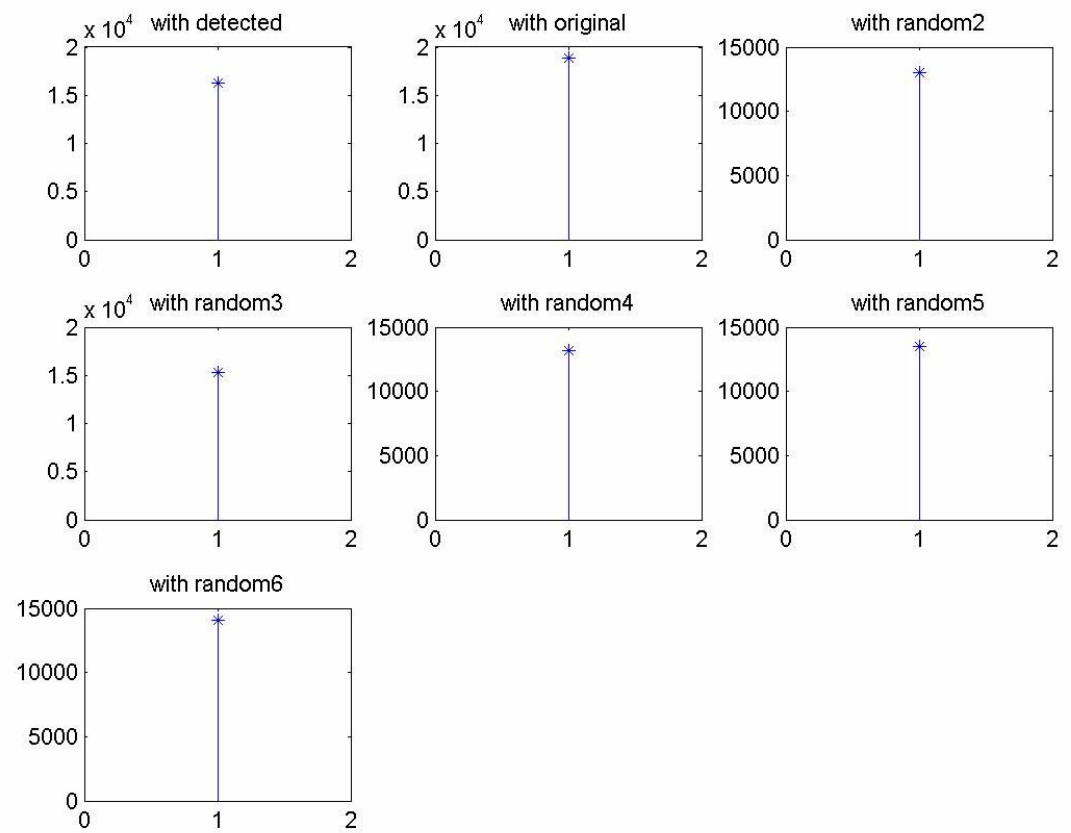
4. noisy_salt_pepper_video



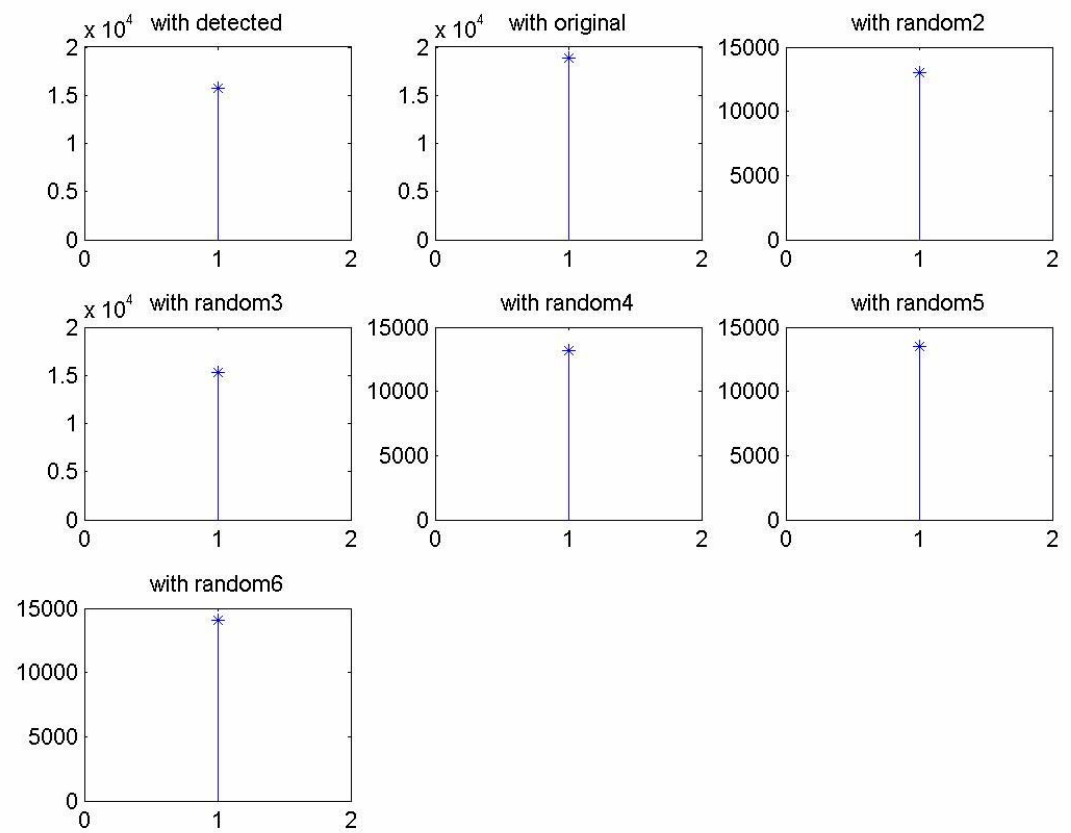
5. averaged_filtered_video



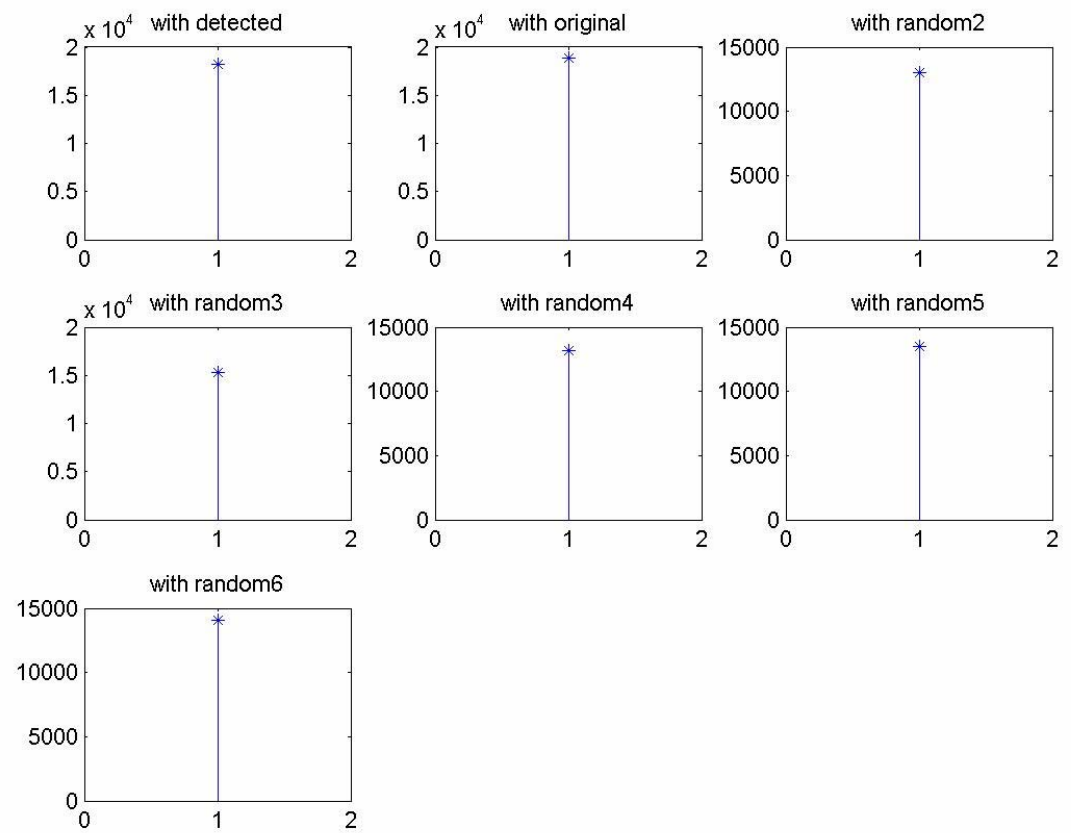
6. median_filtered_video



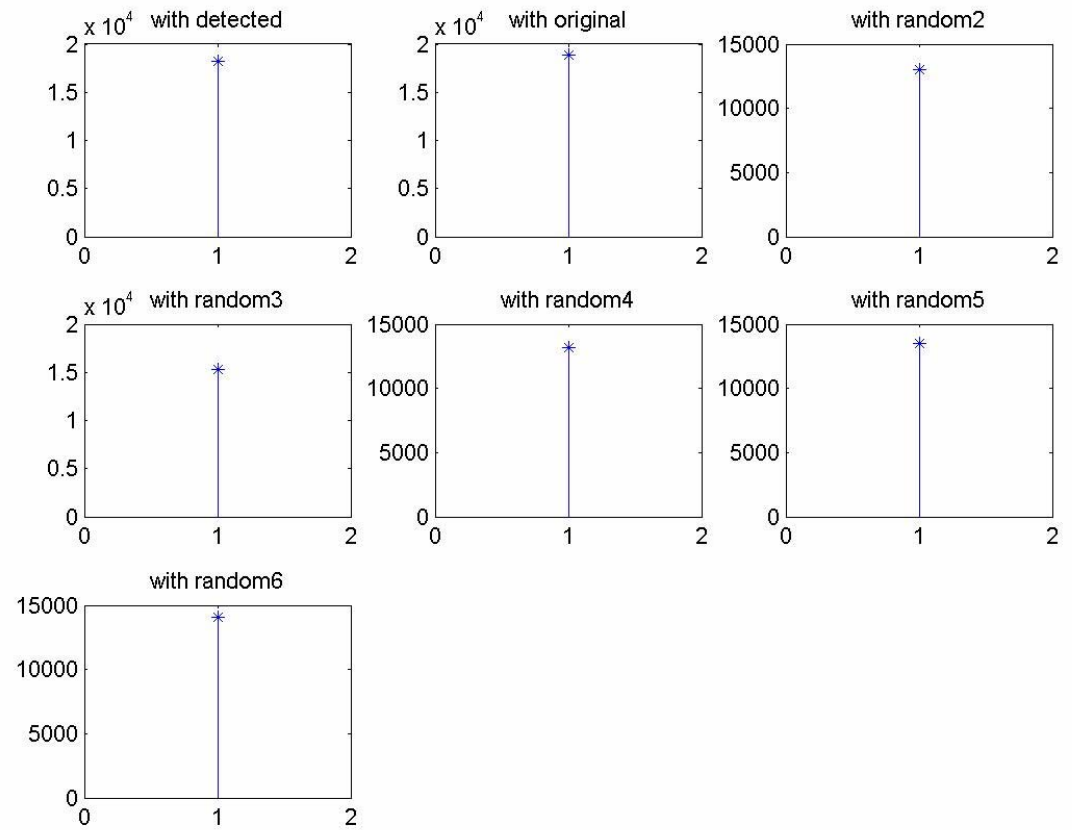
7. wiener_filtered_video



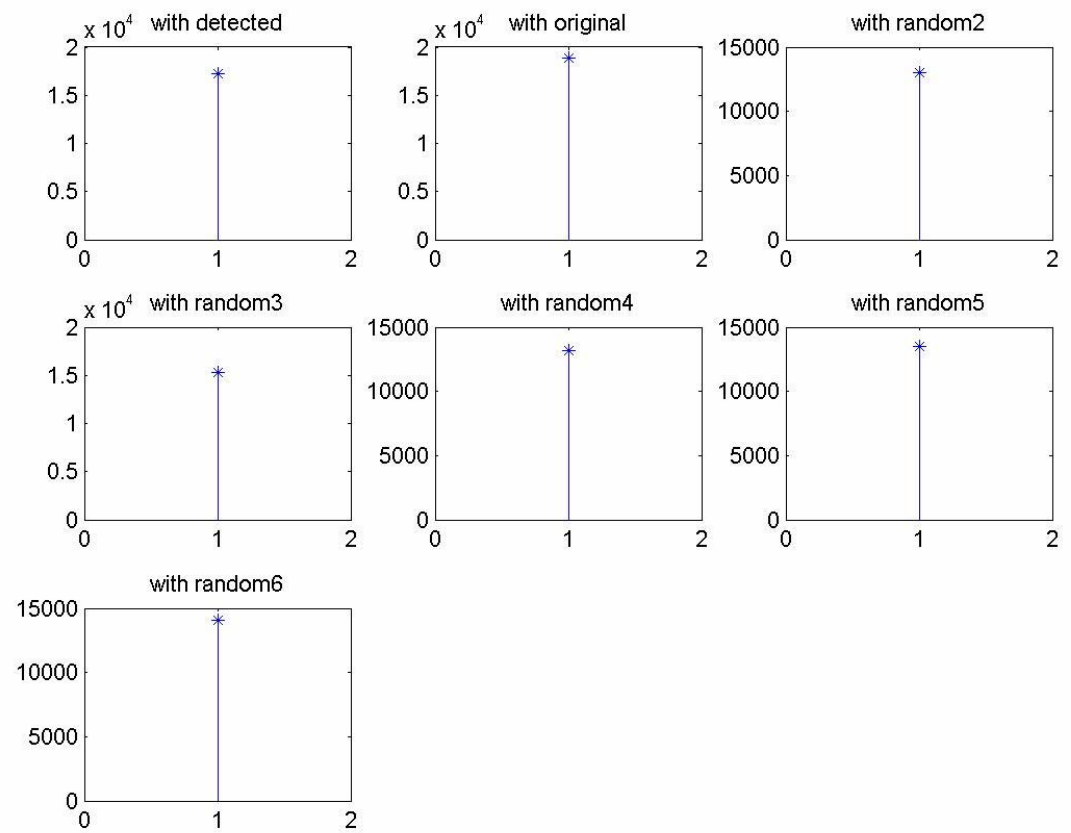
8. pixel_removed_video



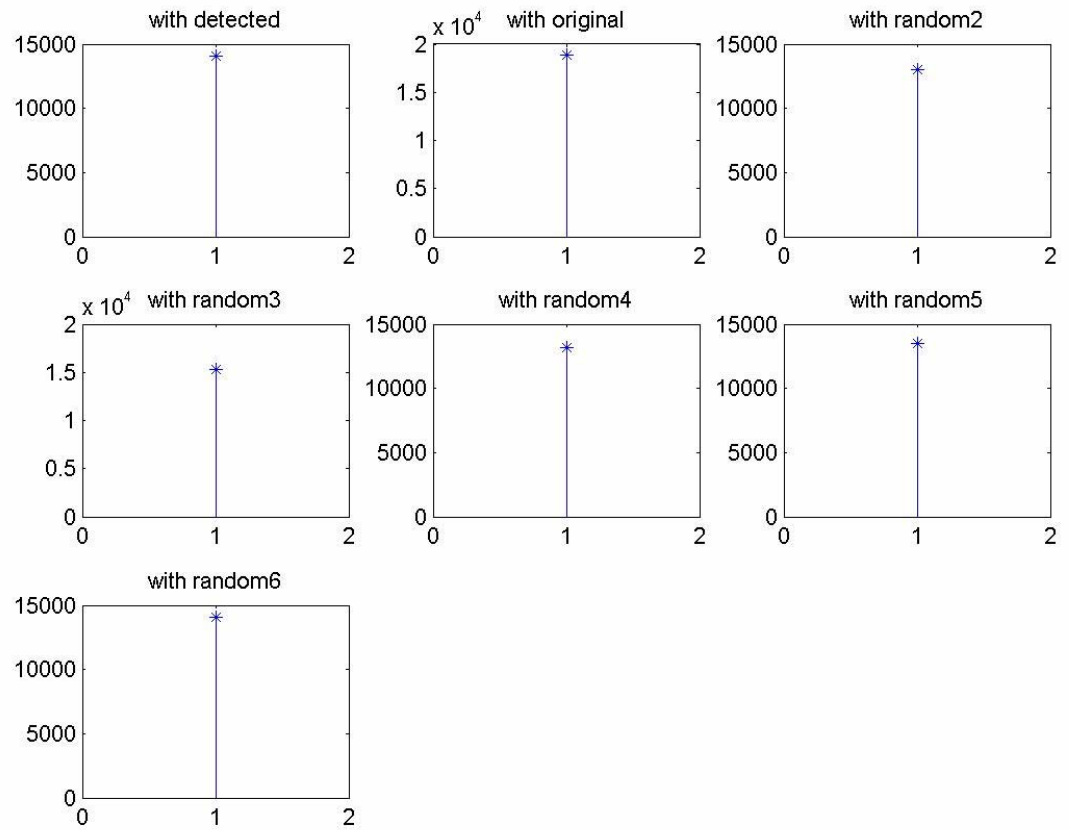
9. line_removed_video



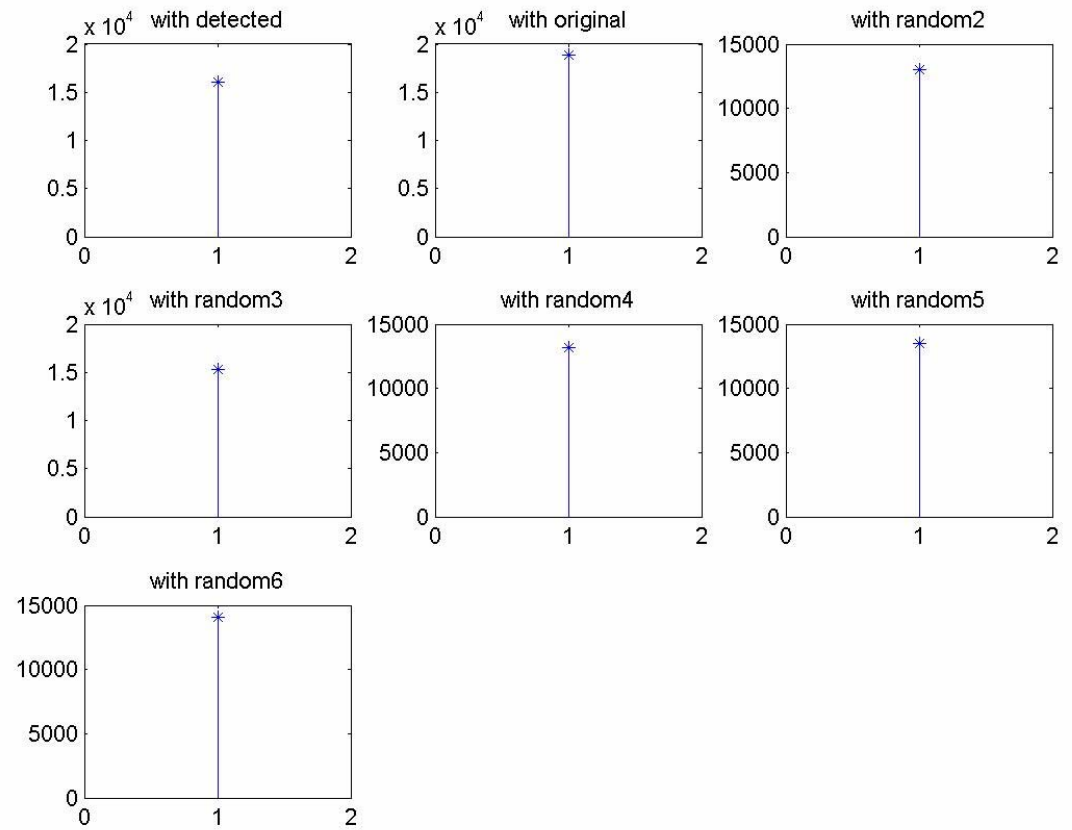
10. frame_removed_video



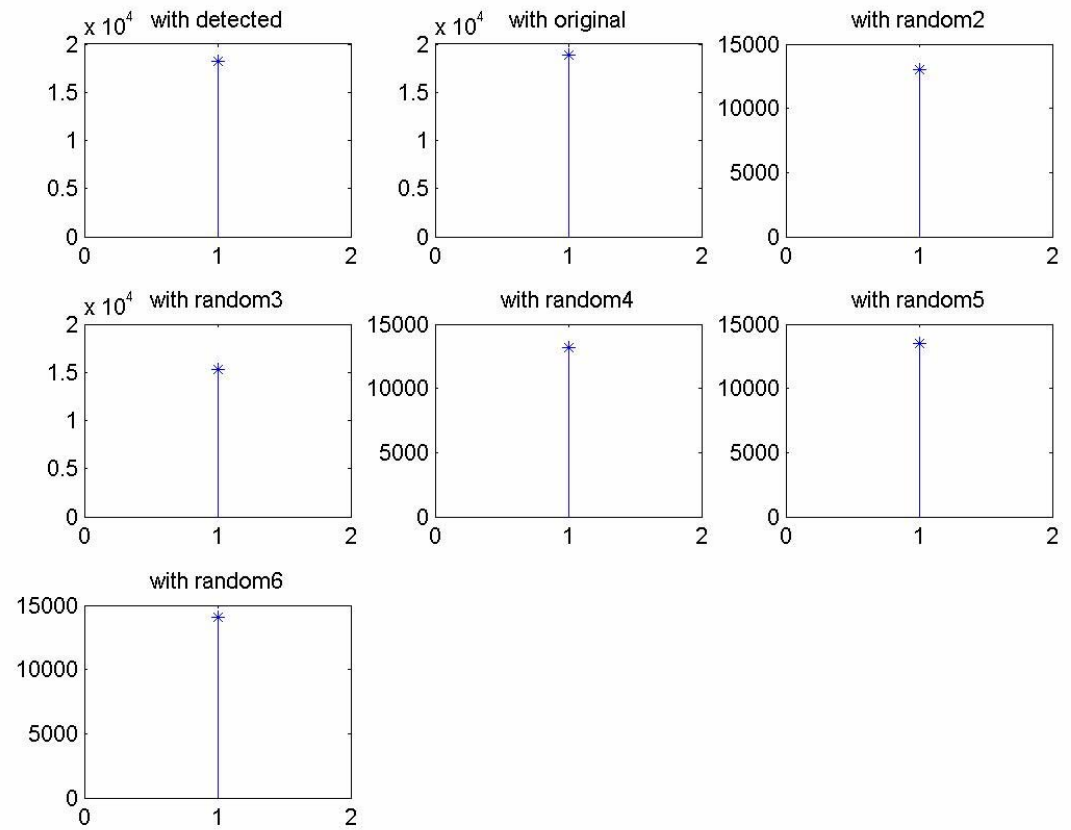
11. frame_rotated_video



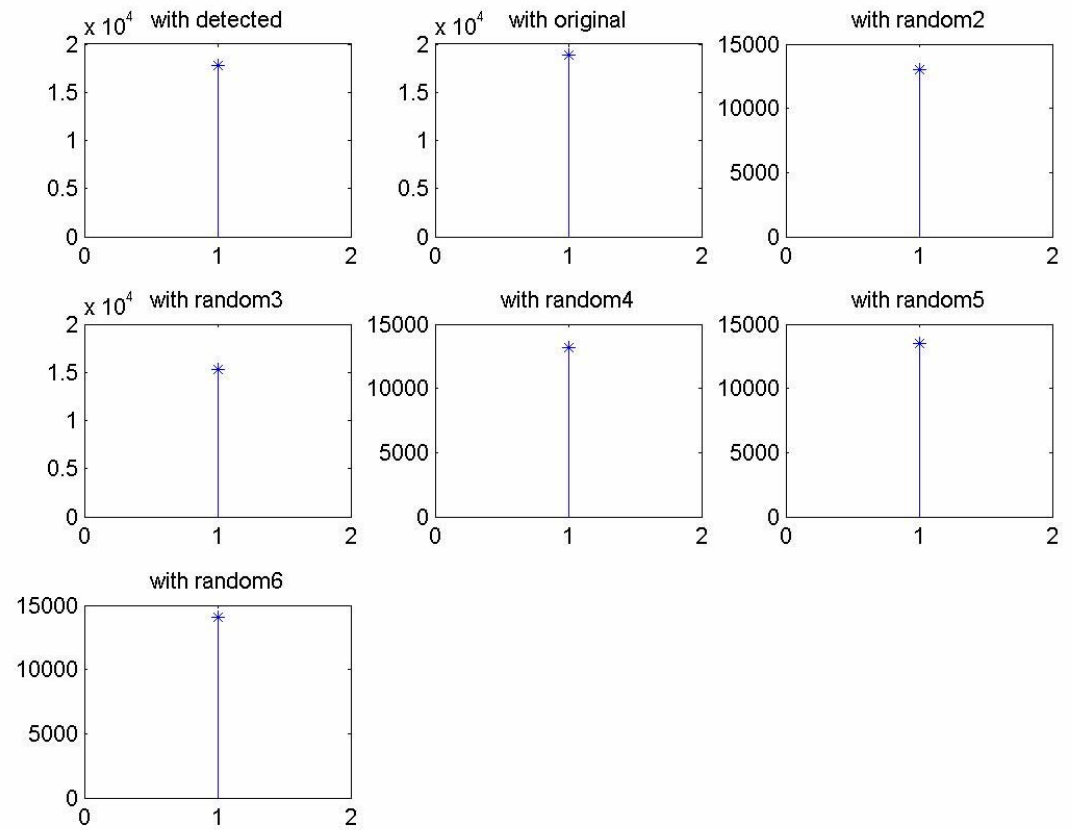
12. frame_dropped_video



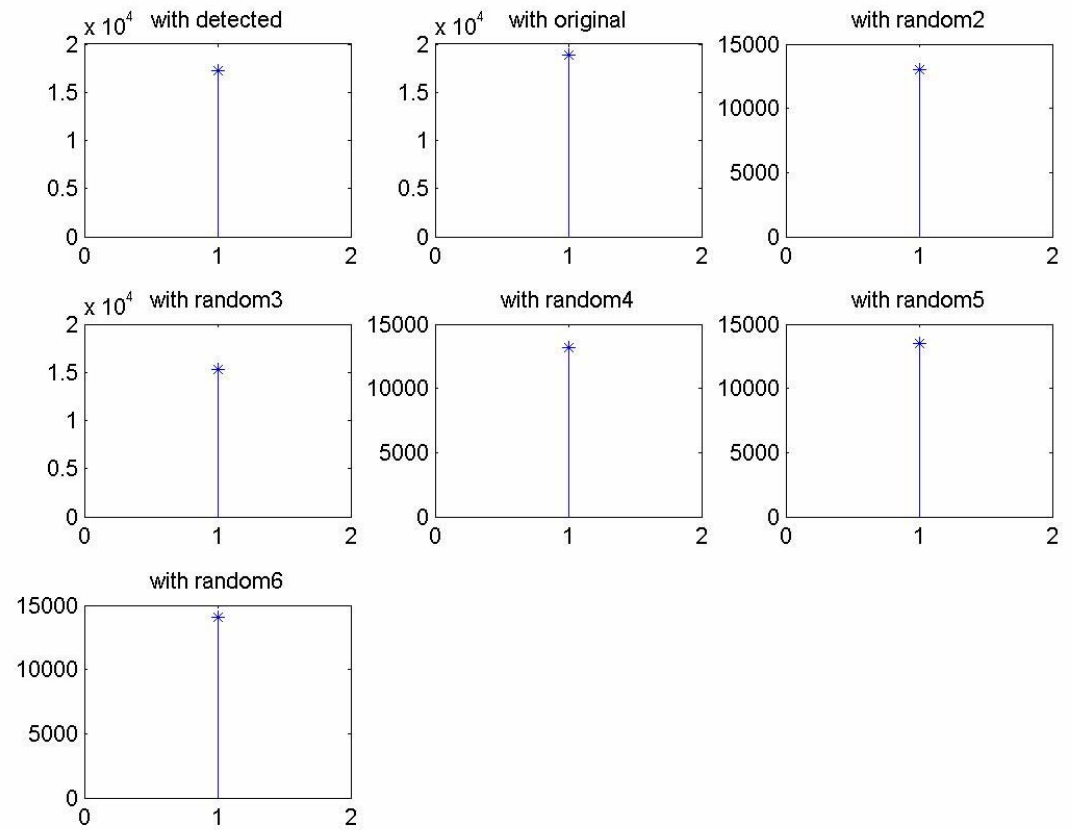
13. frame_swapped_video



14. frame_interpolated_video

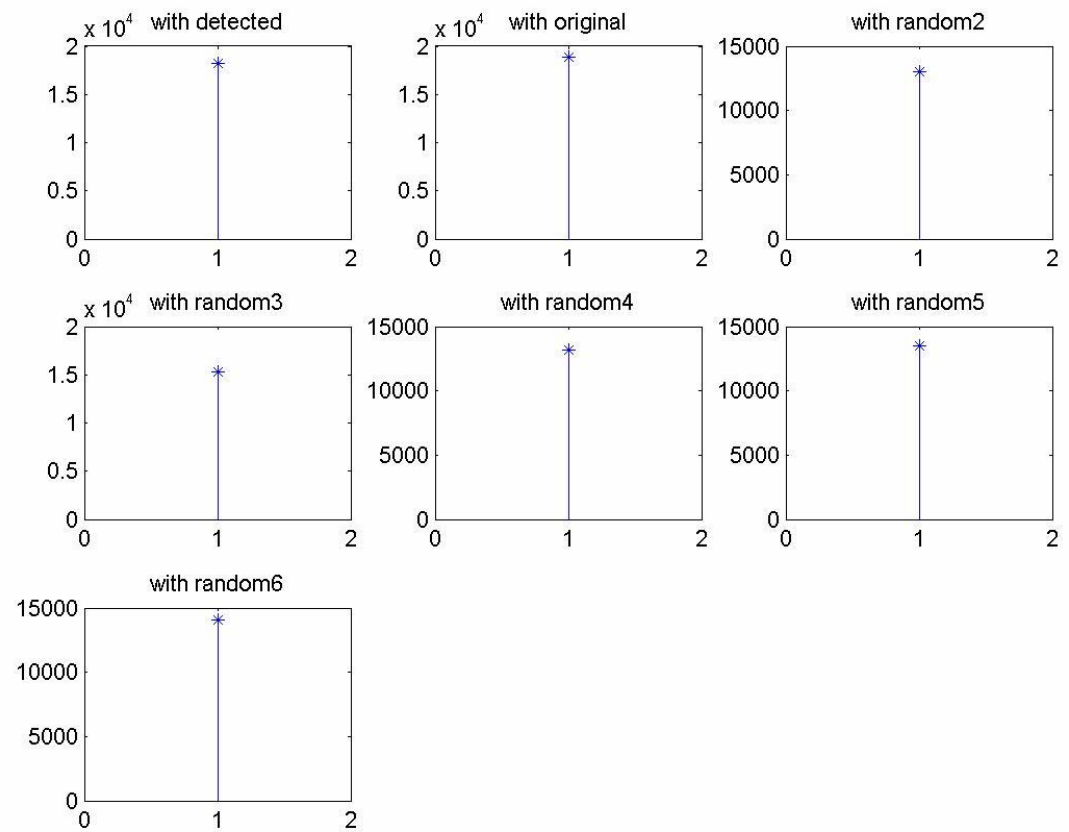


15. frame_resized_video

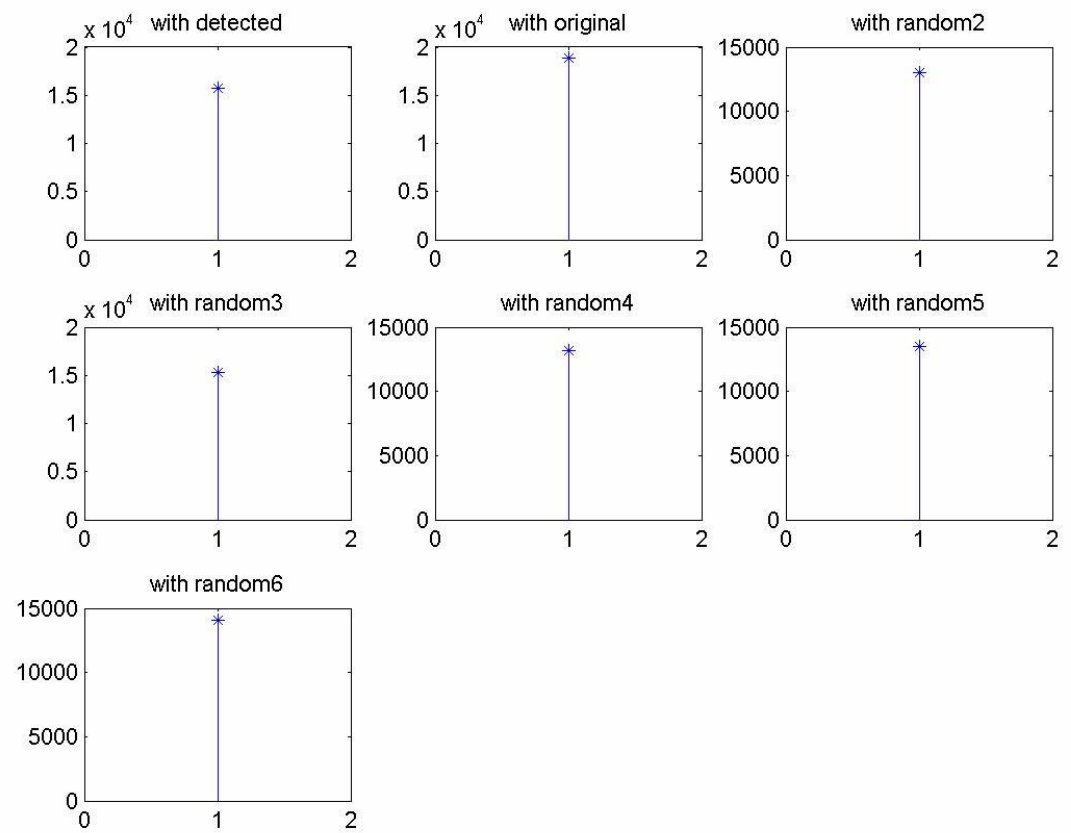


GRAPHICAL DISPLAY OF CORRELATION VALUES (WATERMARKING LSB PLANES)

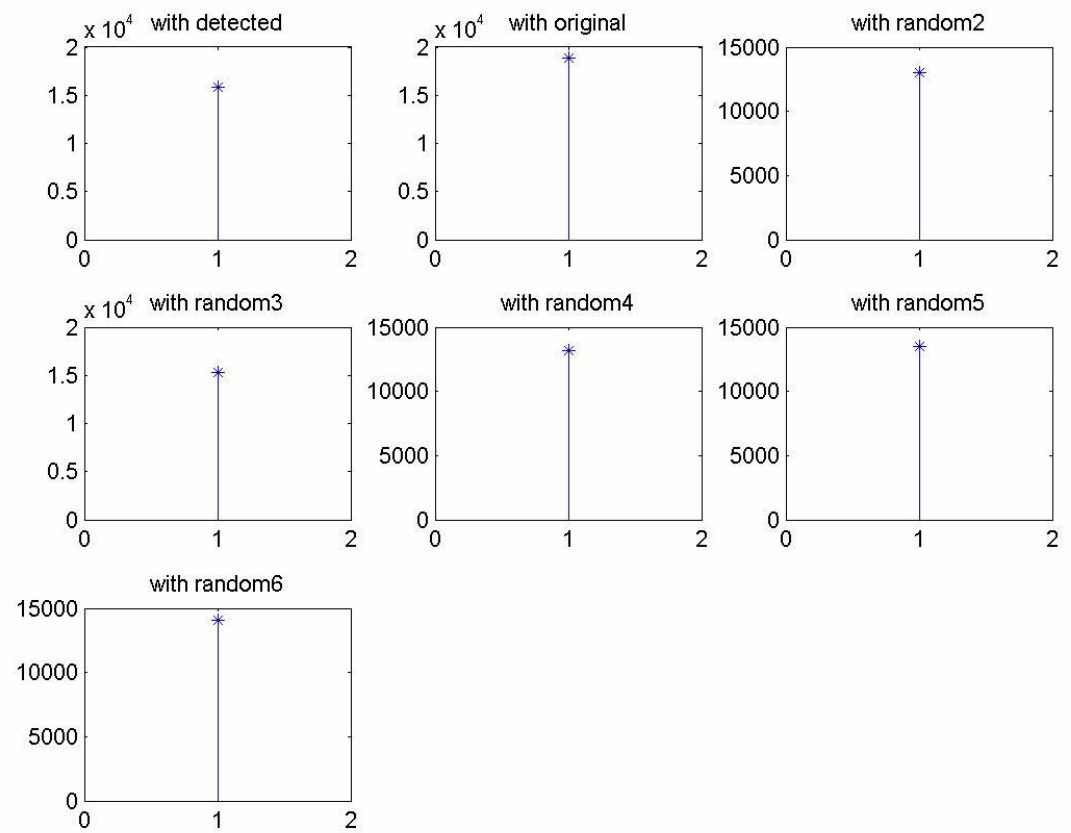
1. watermarked_video



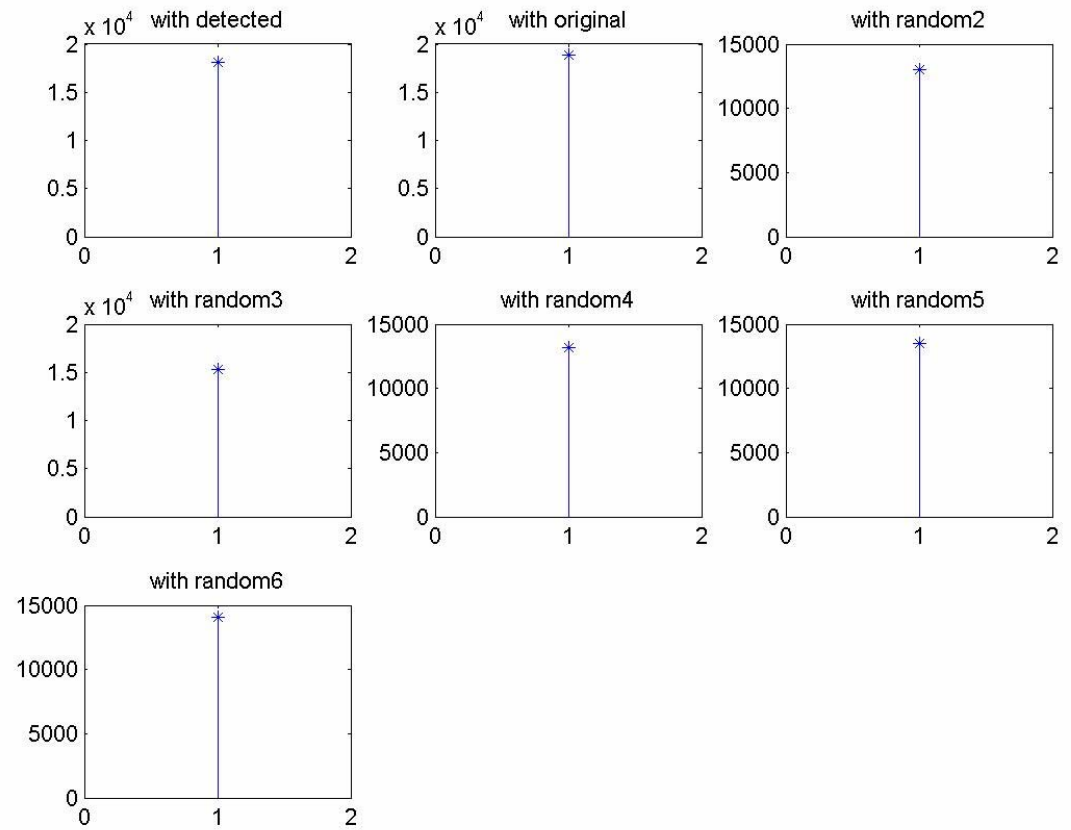
2. compressed_video



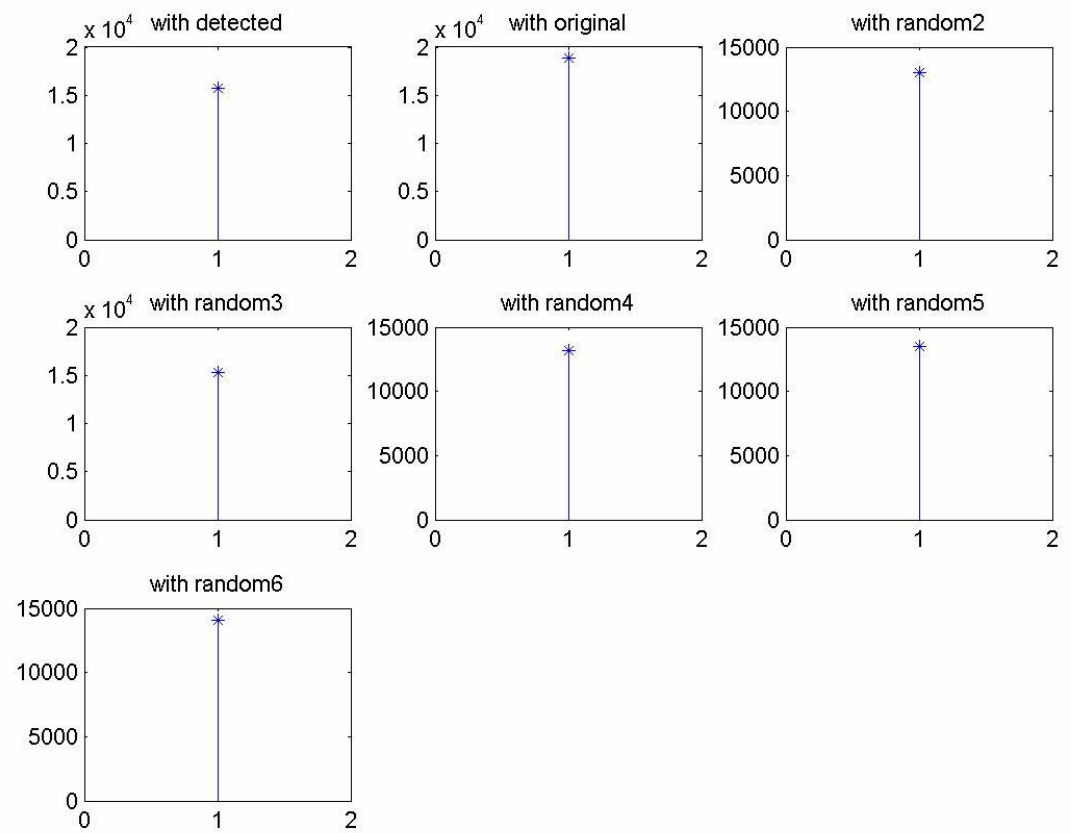
3. noisy_gaussian_video



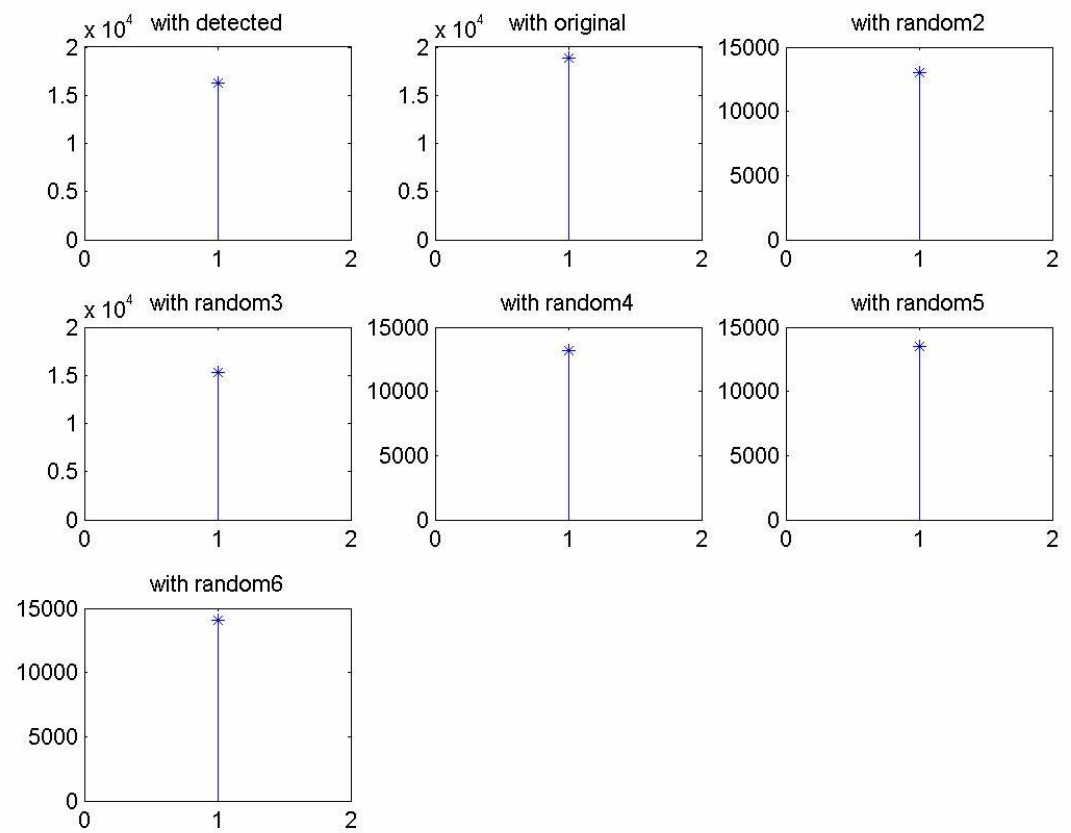
4. noisy_salt_pepper_video



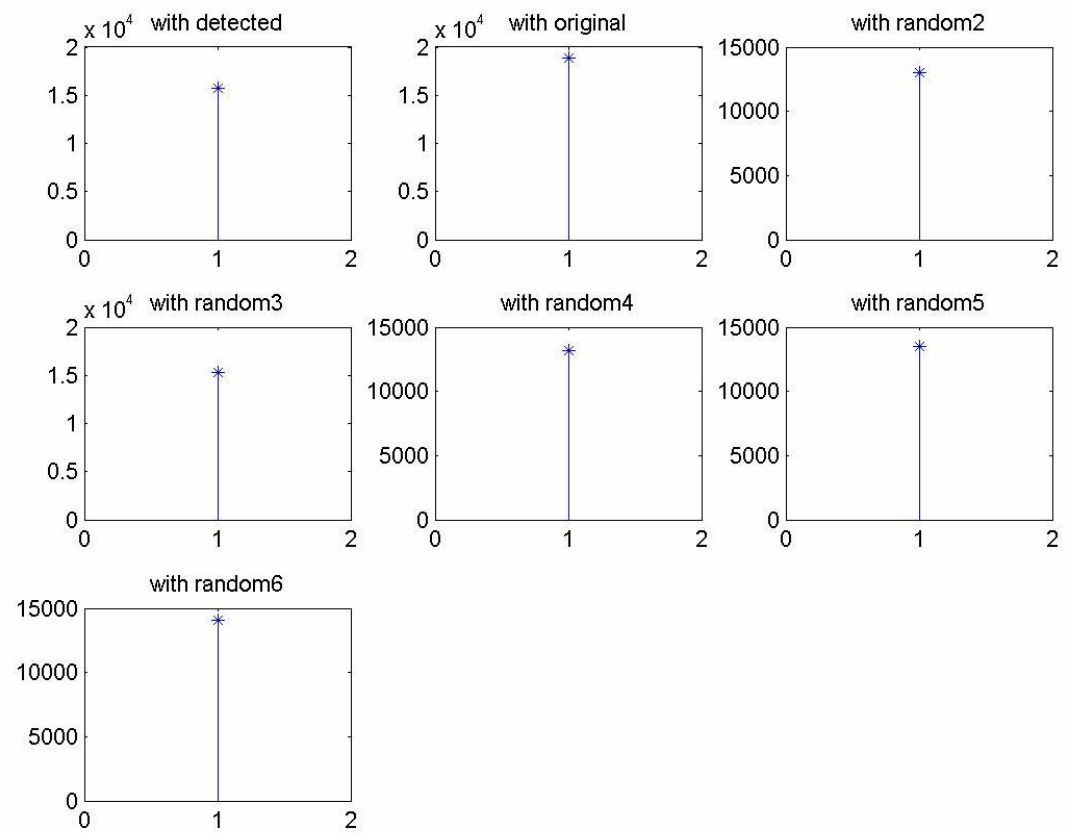
5. averaged_filtered_video



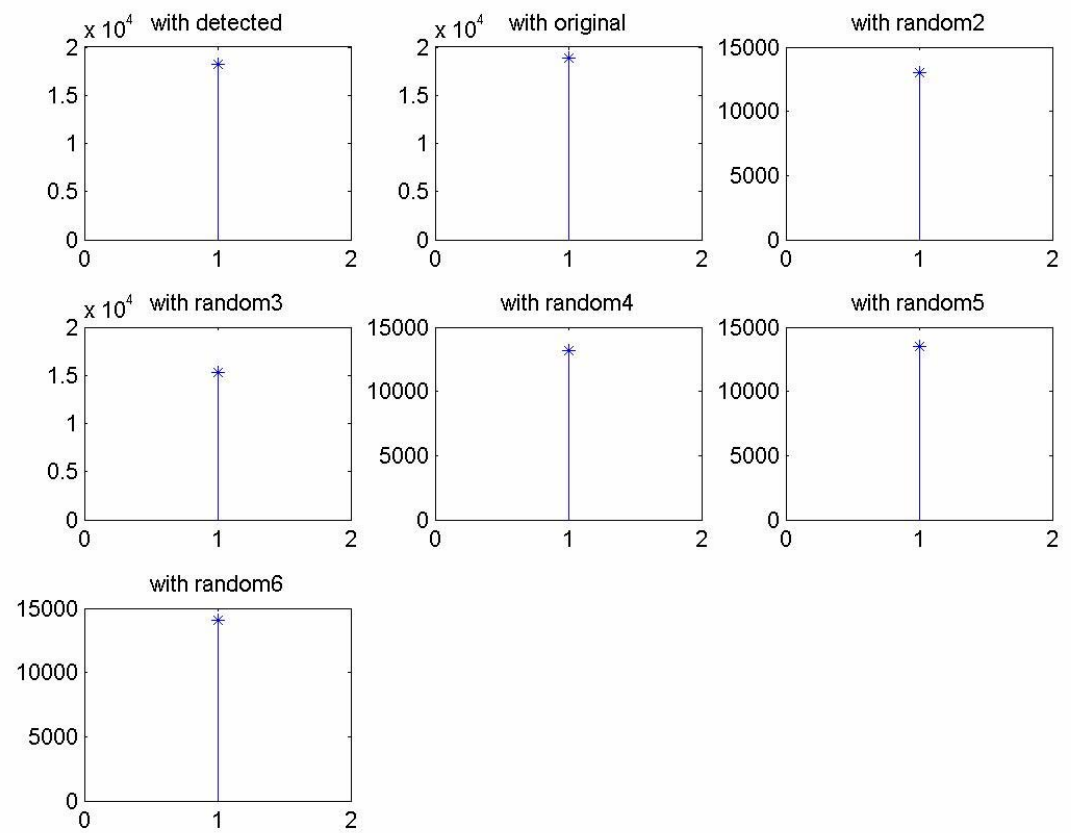
6. median_filtered_video



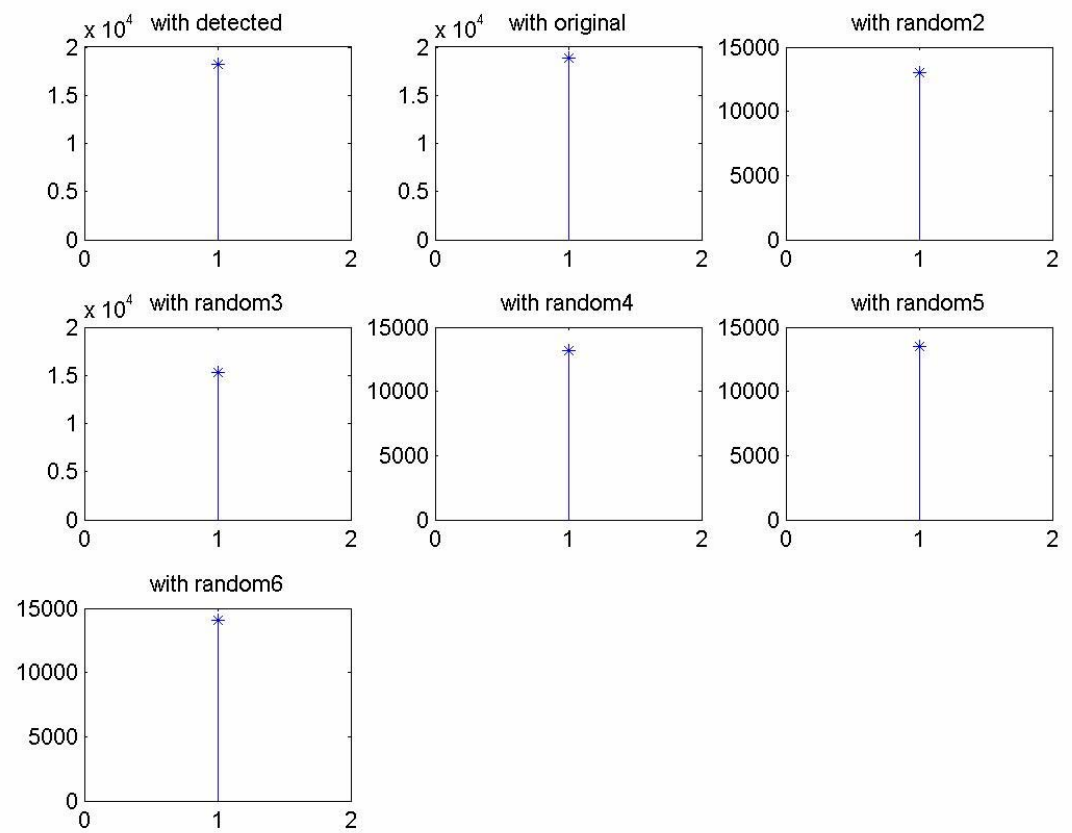
7. wiener_filtered_video



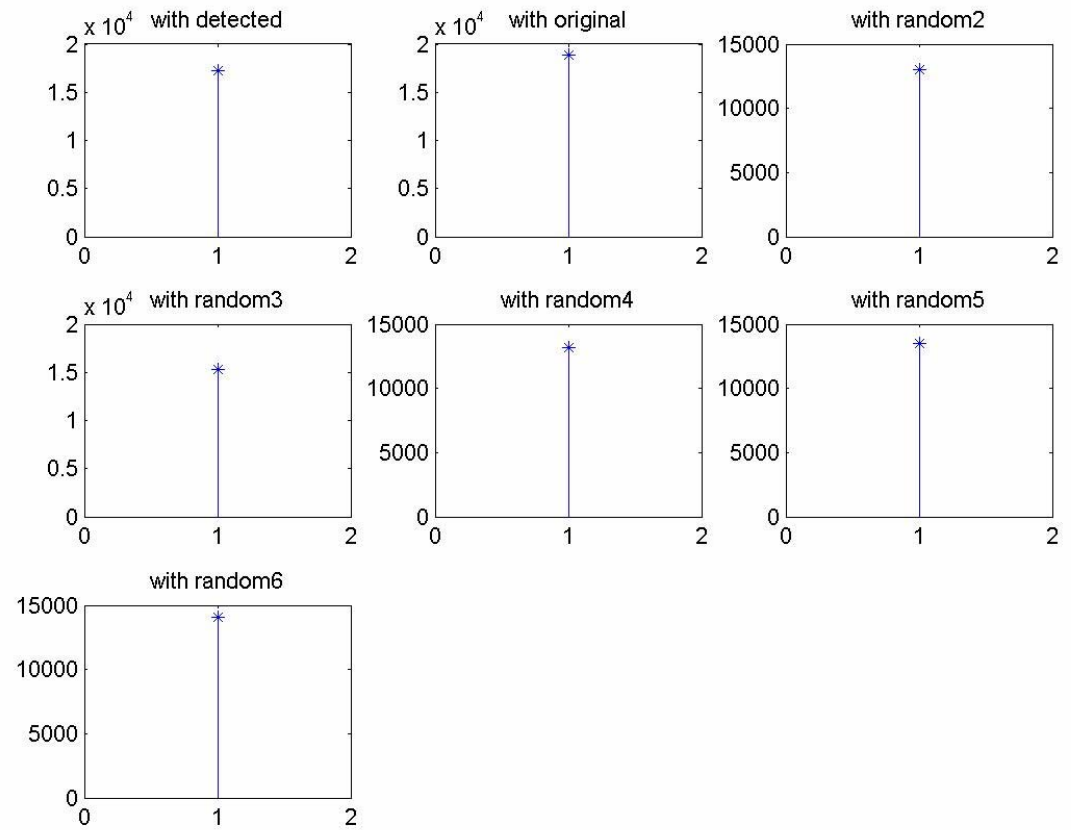
8. pixel_removed_video



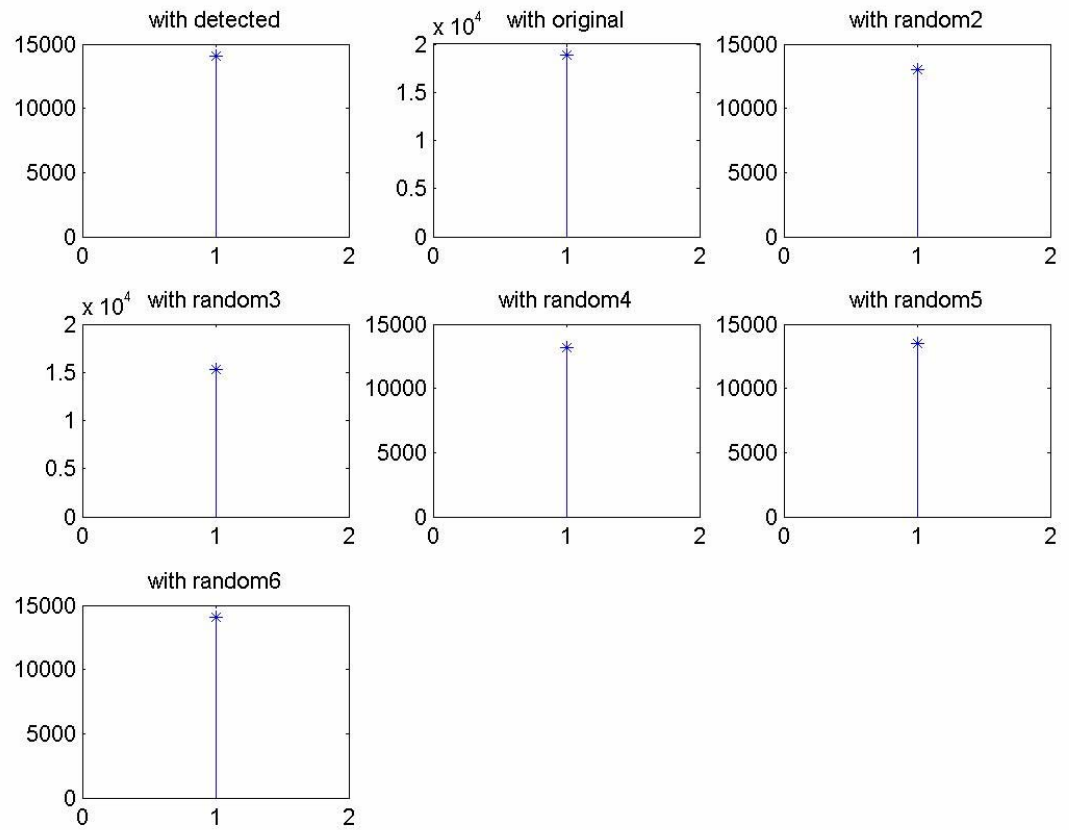
9. line_removed_video



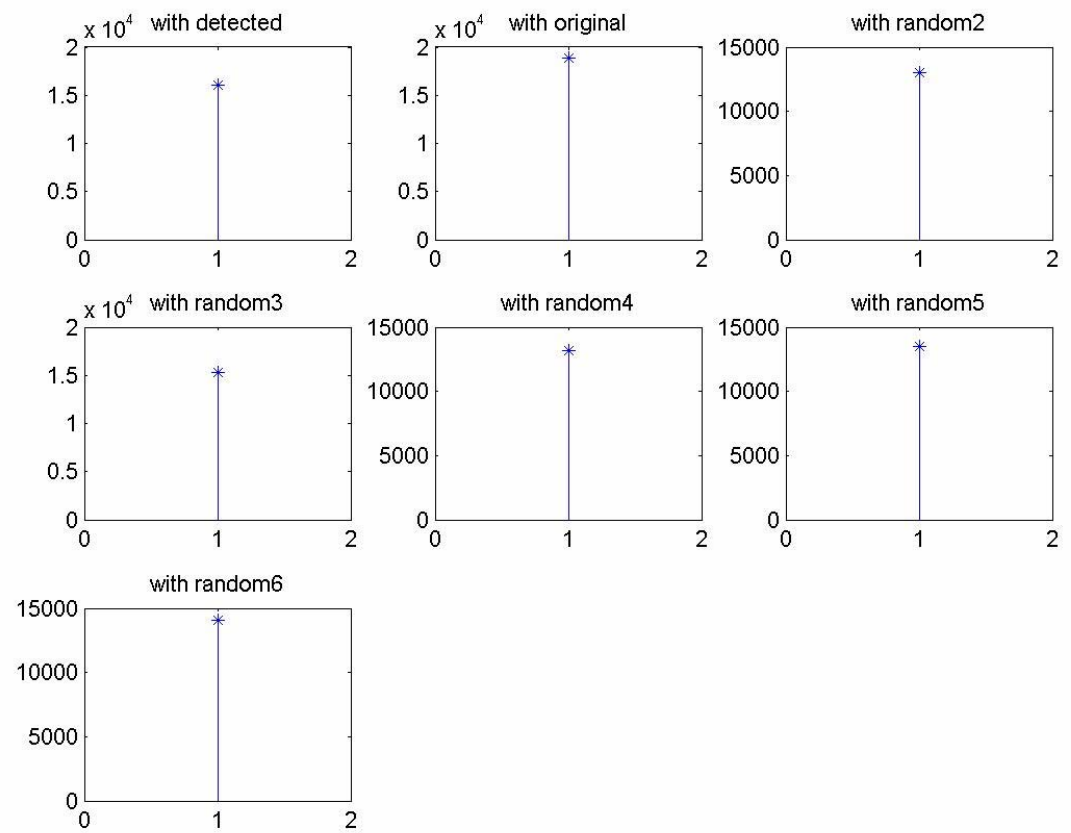
10. frame_removed_video



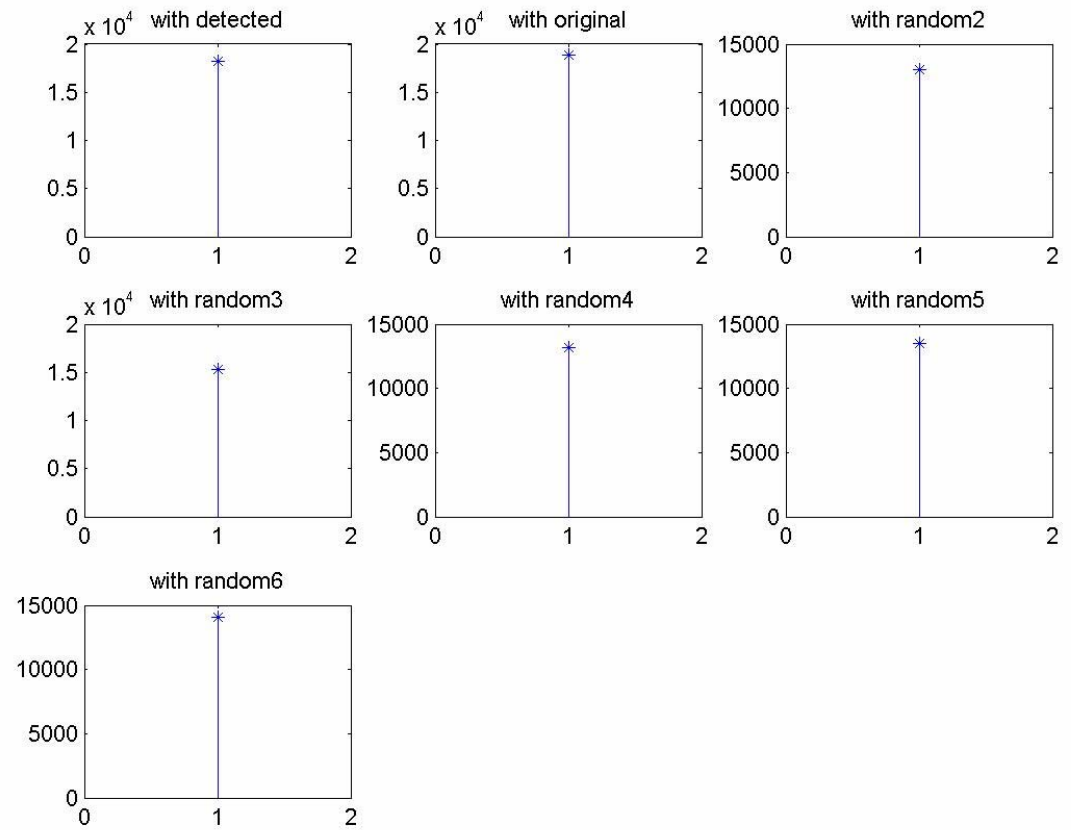
11. frame_rotated_video



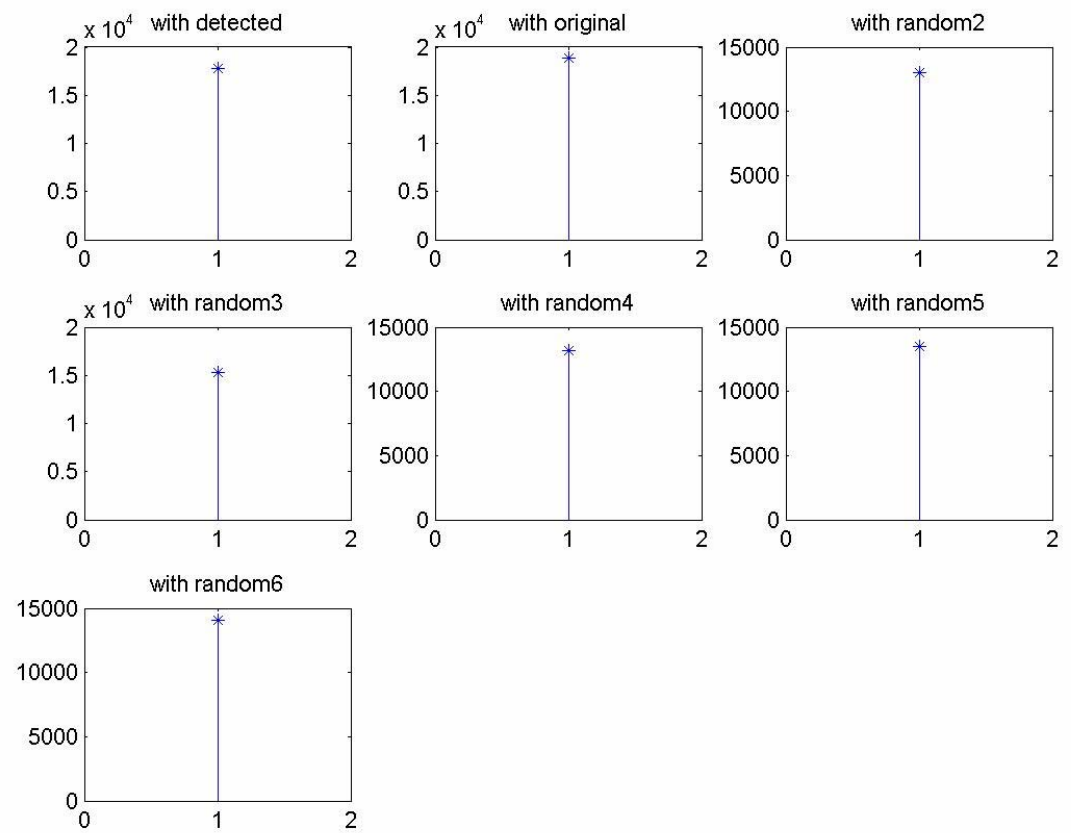
12. frame_dropped_video



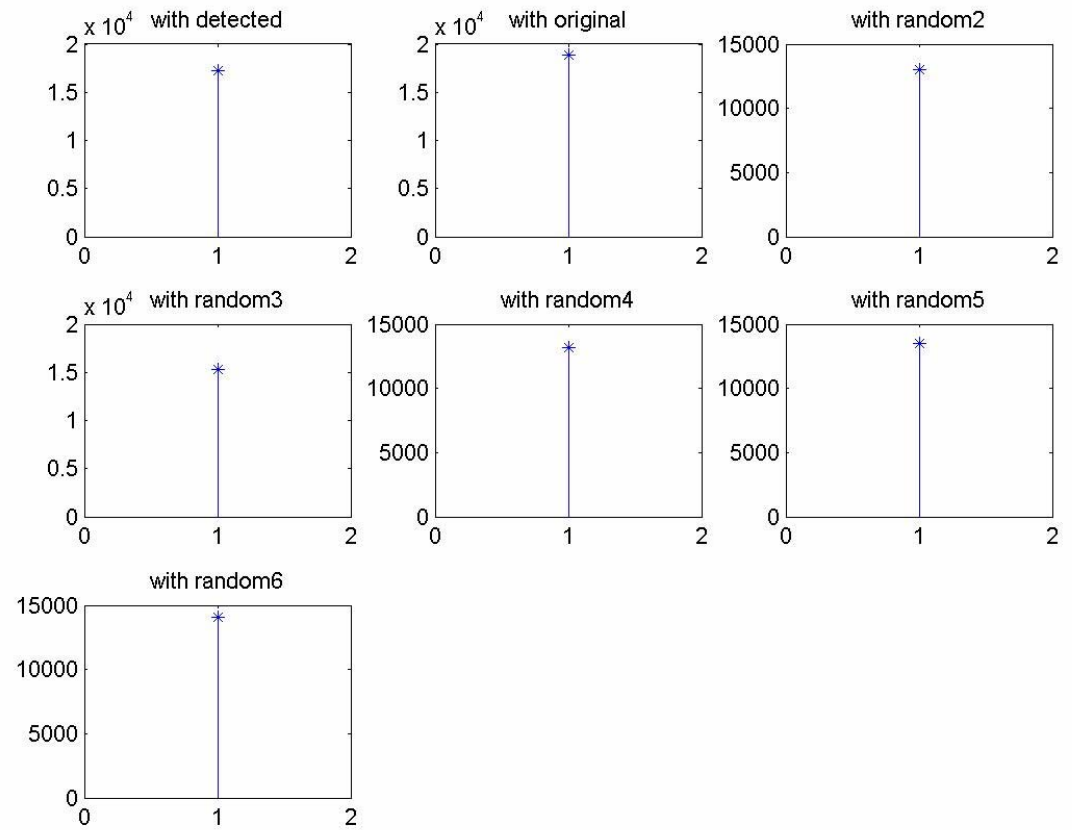
13. frame_swapped_video



14. frame_interpolated_video

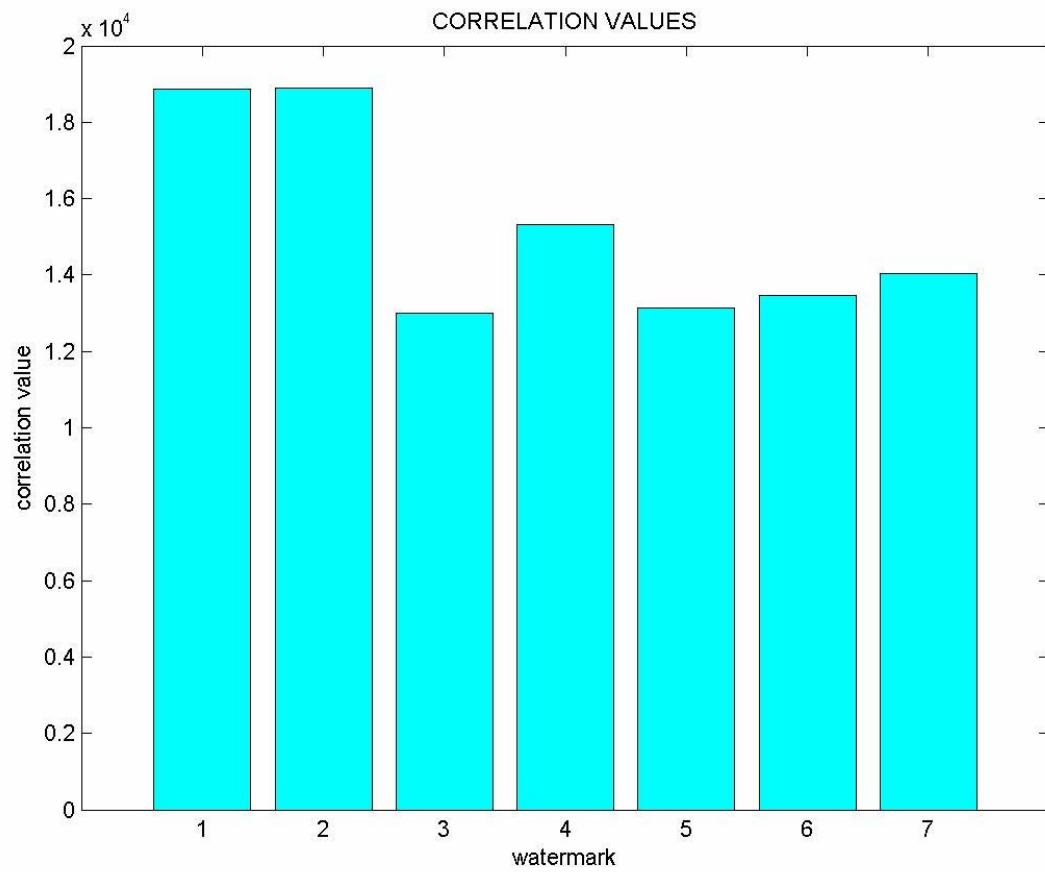


15. frame_resized_video

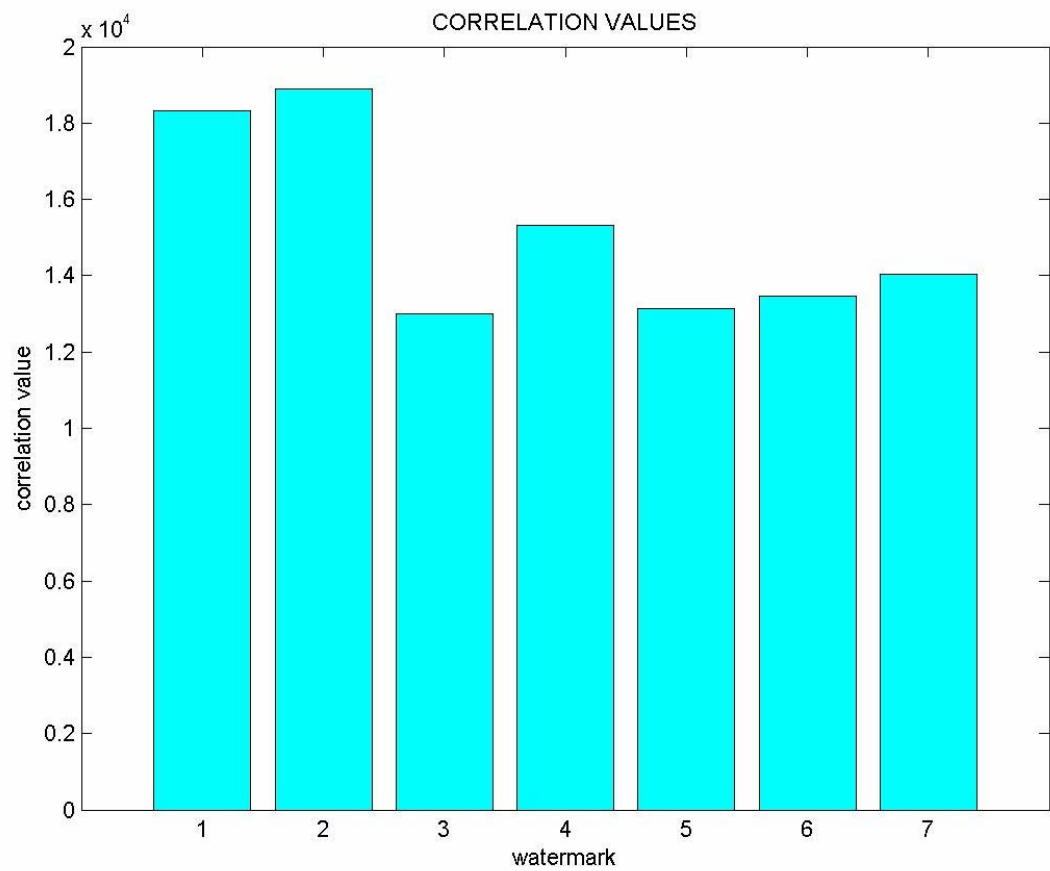


COMPARISON ON THE BASIS OF CORRELATION VALUES (WATERMARKING MSB PLANES)

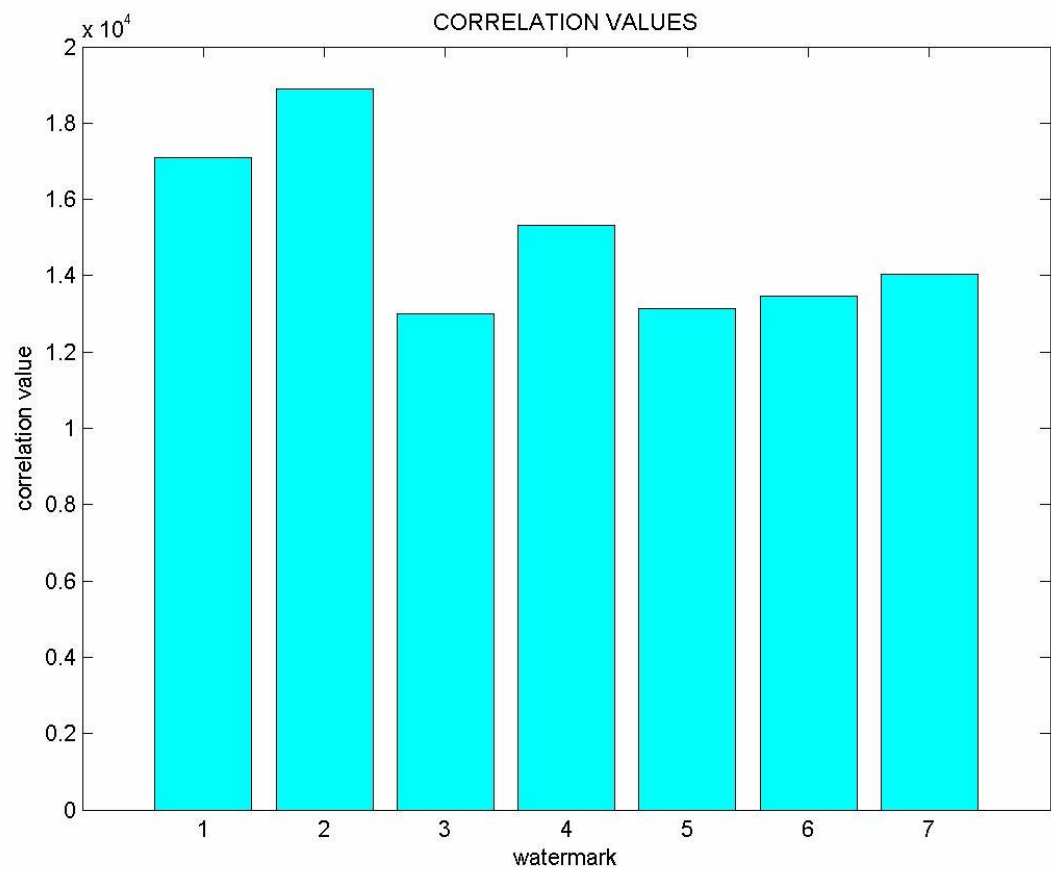
1. watermarked_video



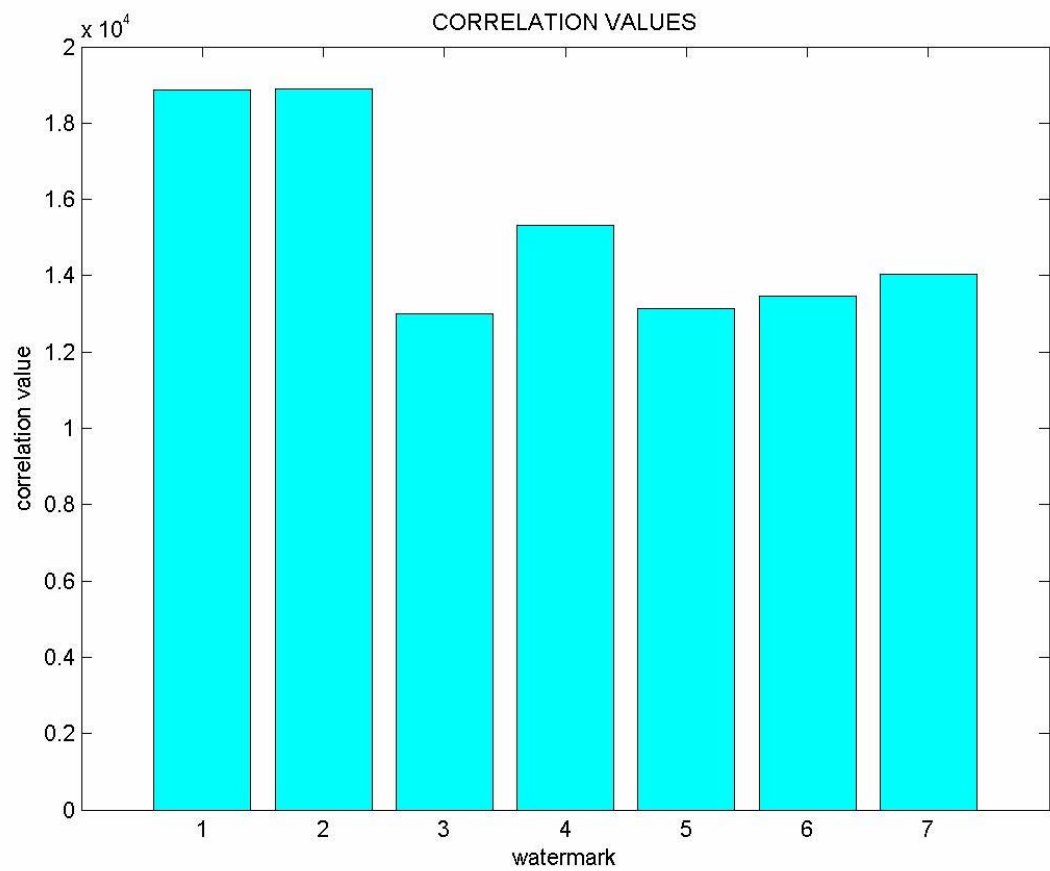
2. compressed_video



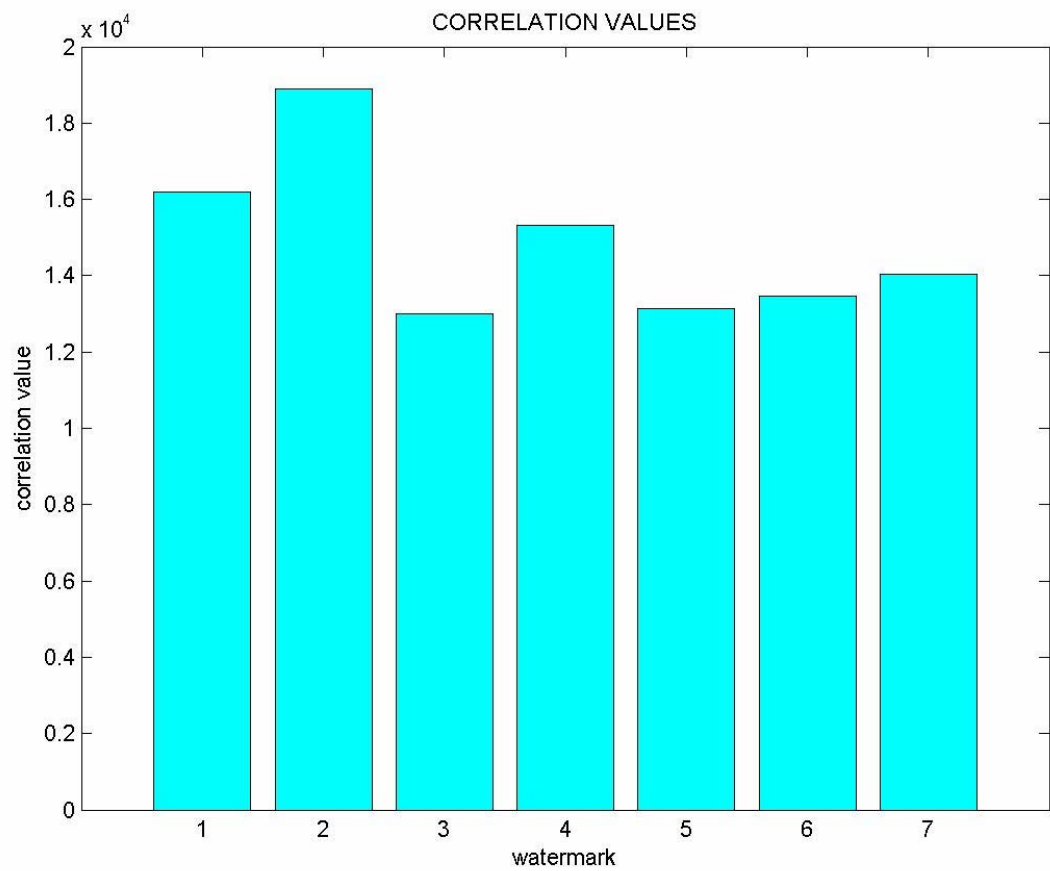
3. noisy_gaussian_video



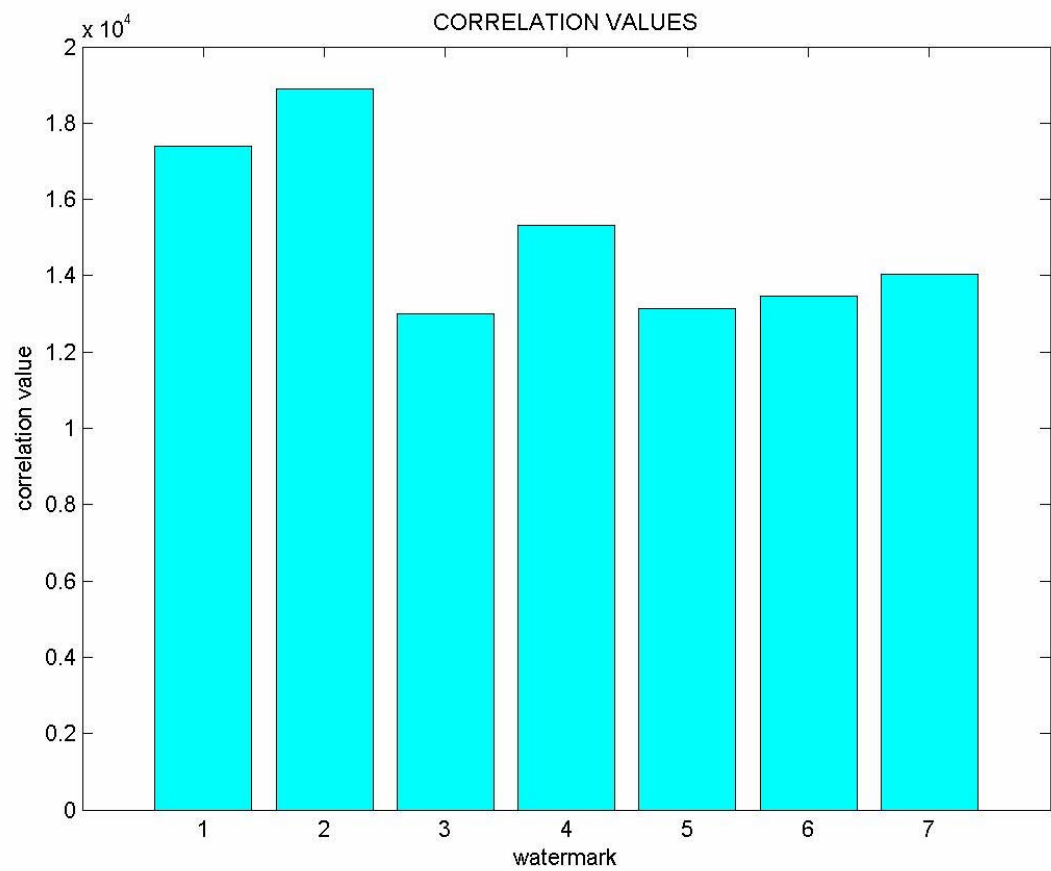
4. noisy_salt_pepper_video



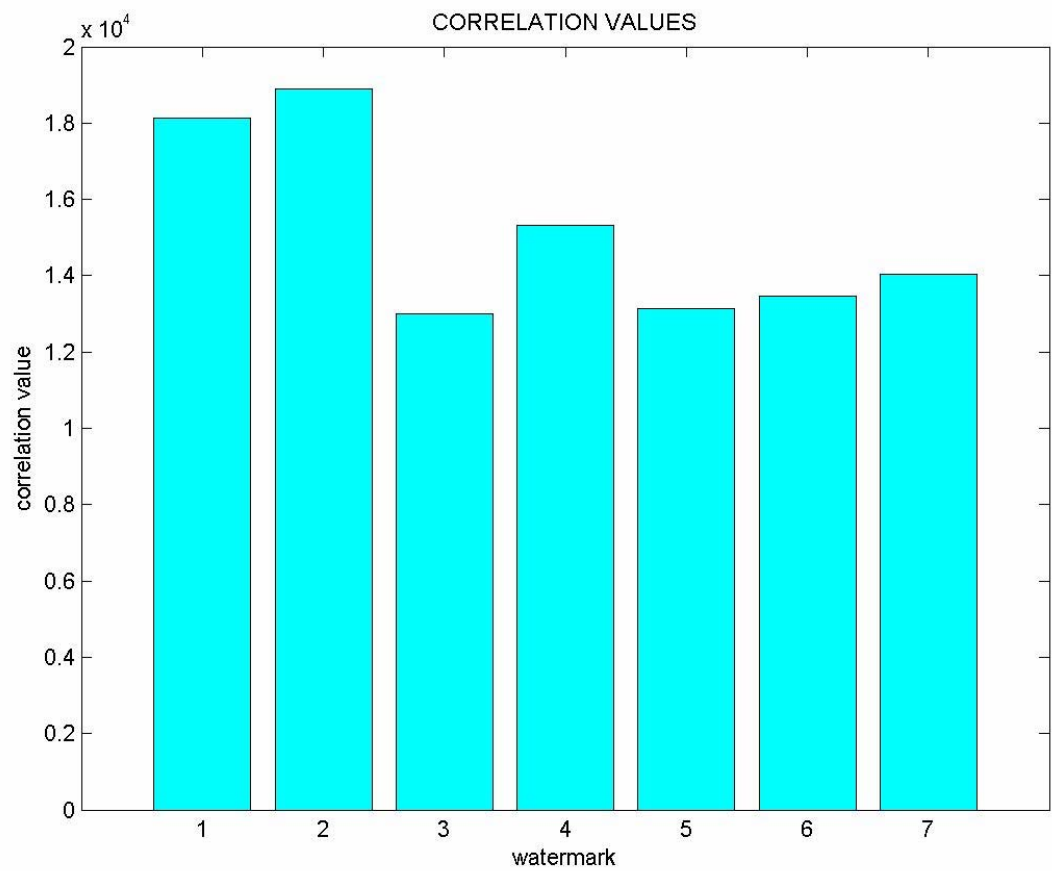
5. averaged_filtered_video



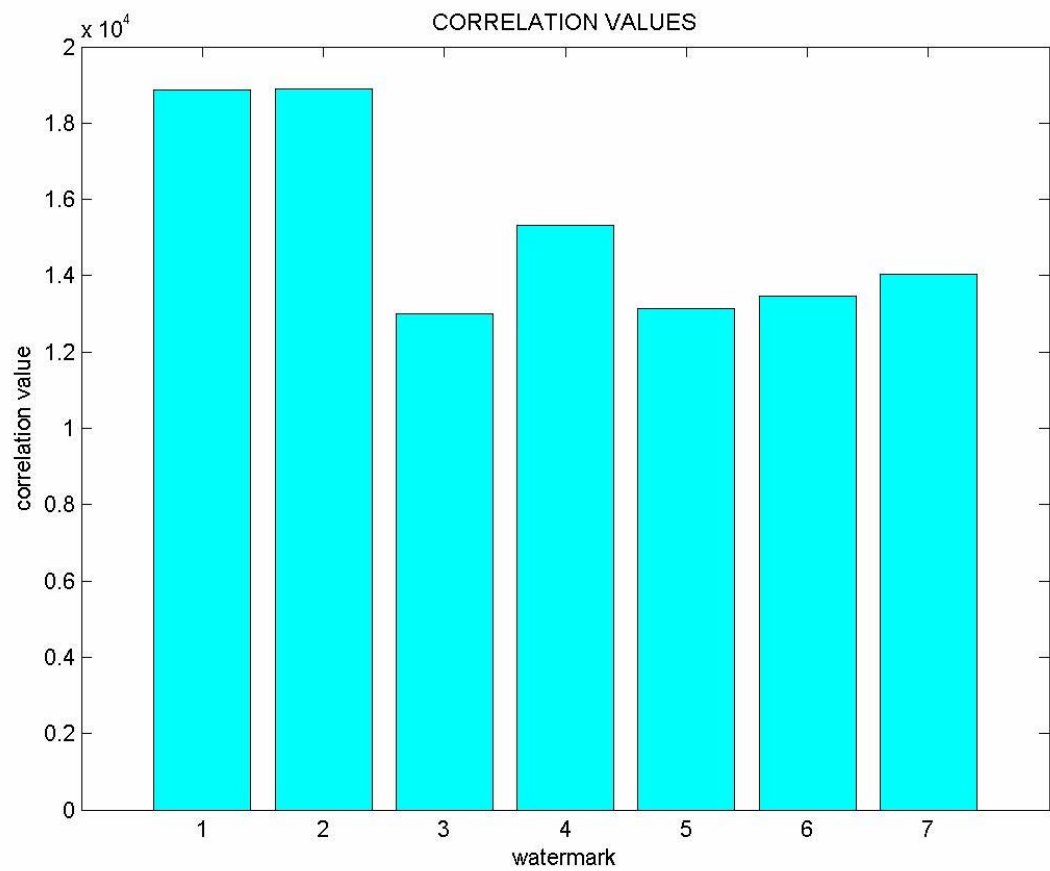
6. median_filtered_video



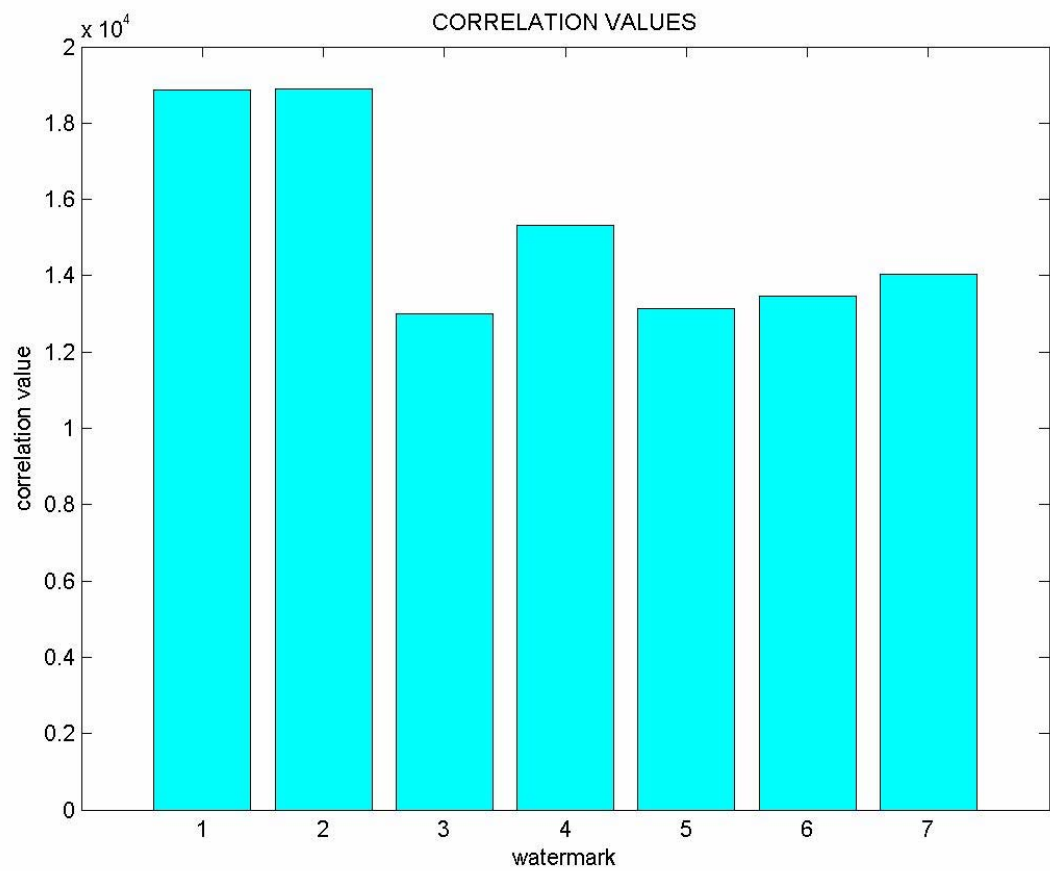
7. wiener_filtered_video



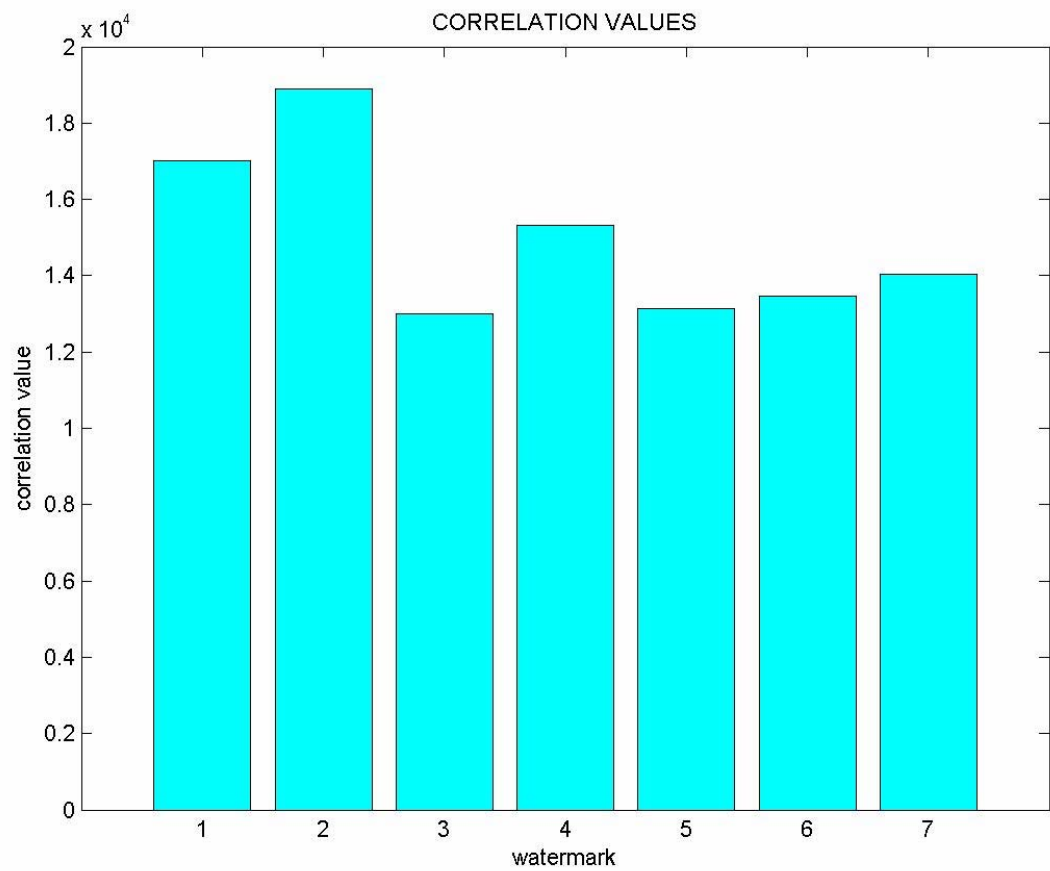
8. pixel_removed_video



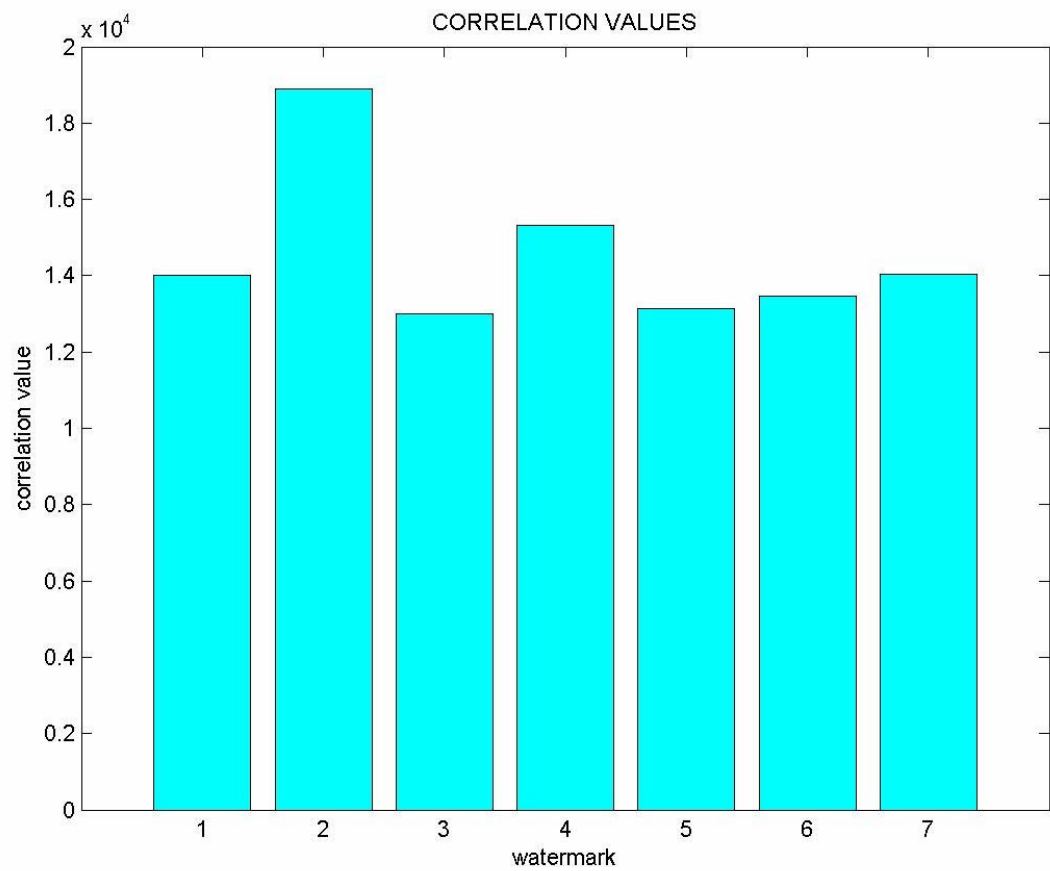
9. line_removed_video



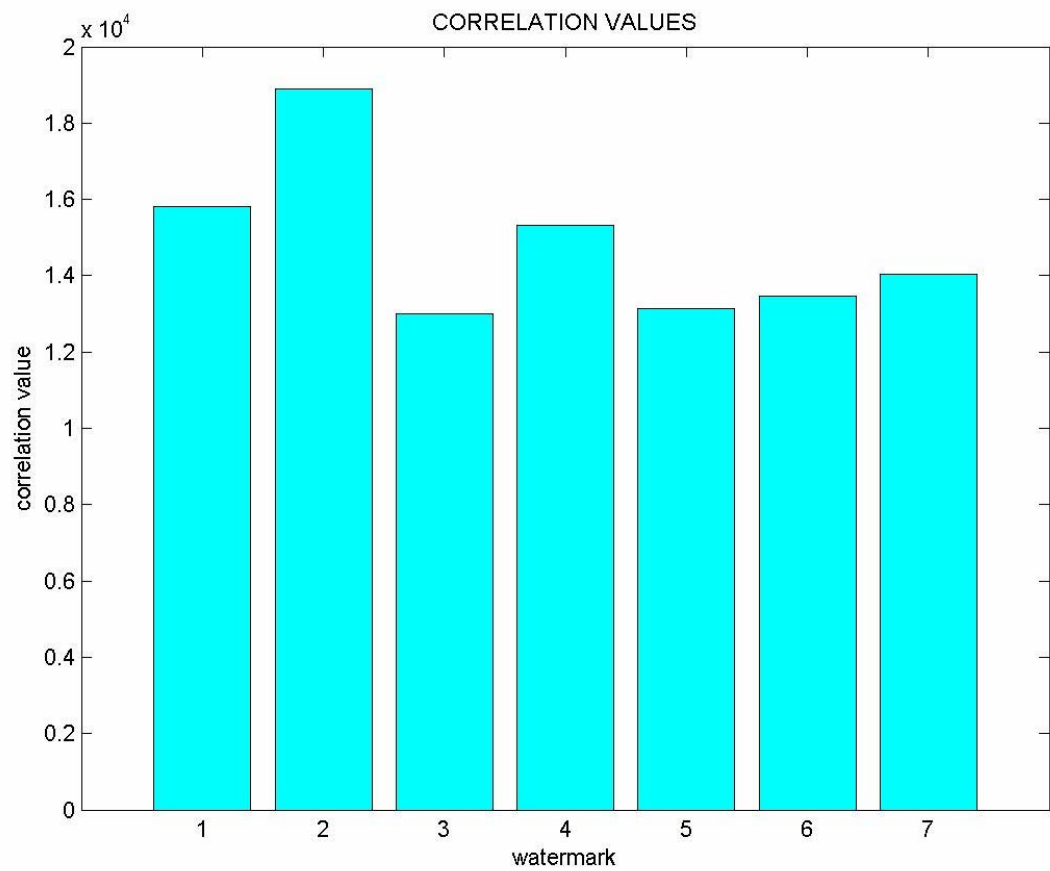
10. frame_removed_video



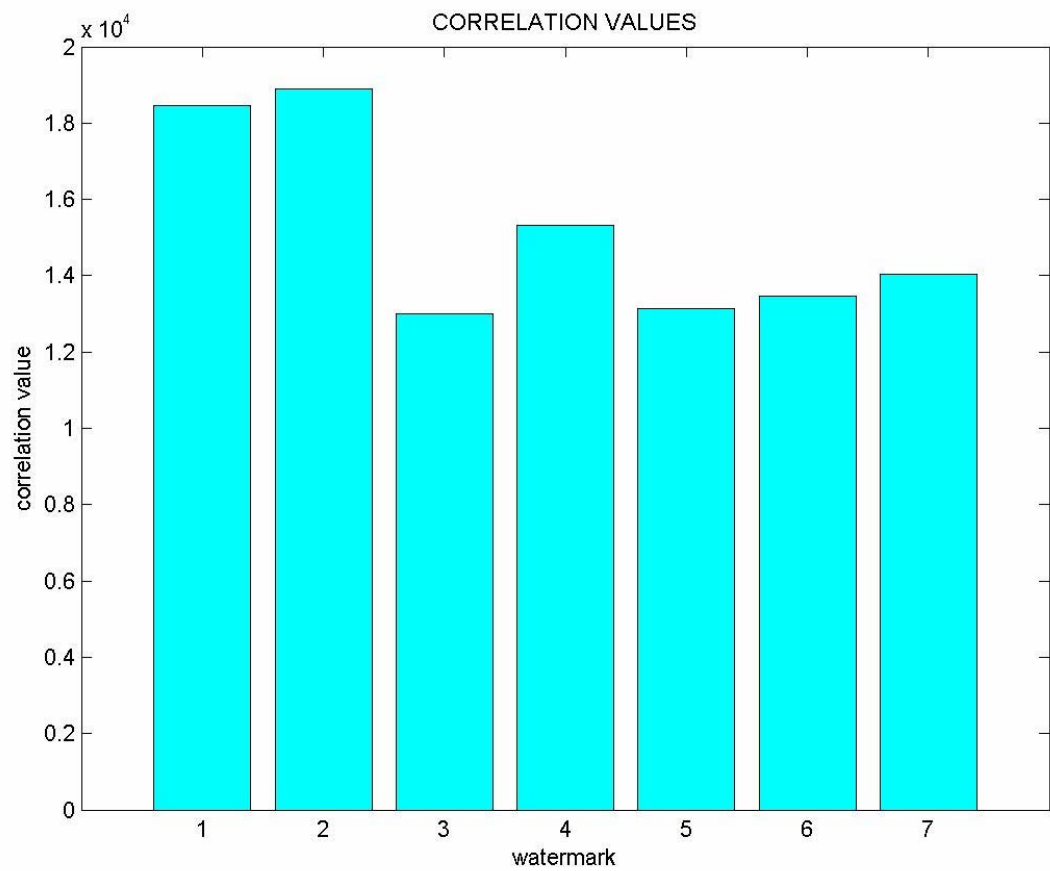
11. frame_rotated_video



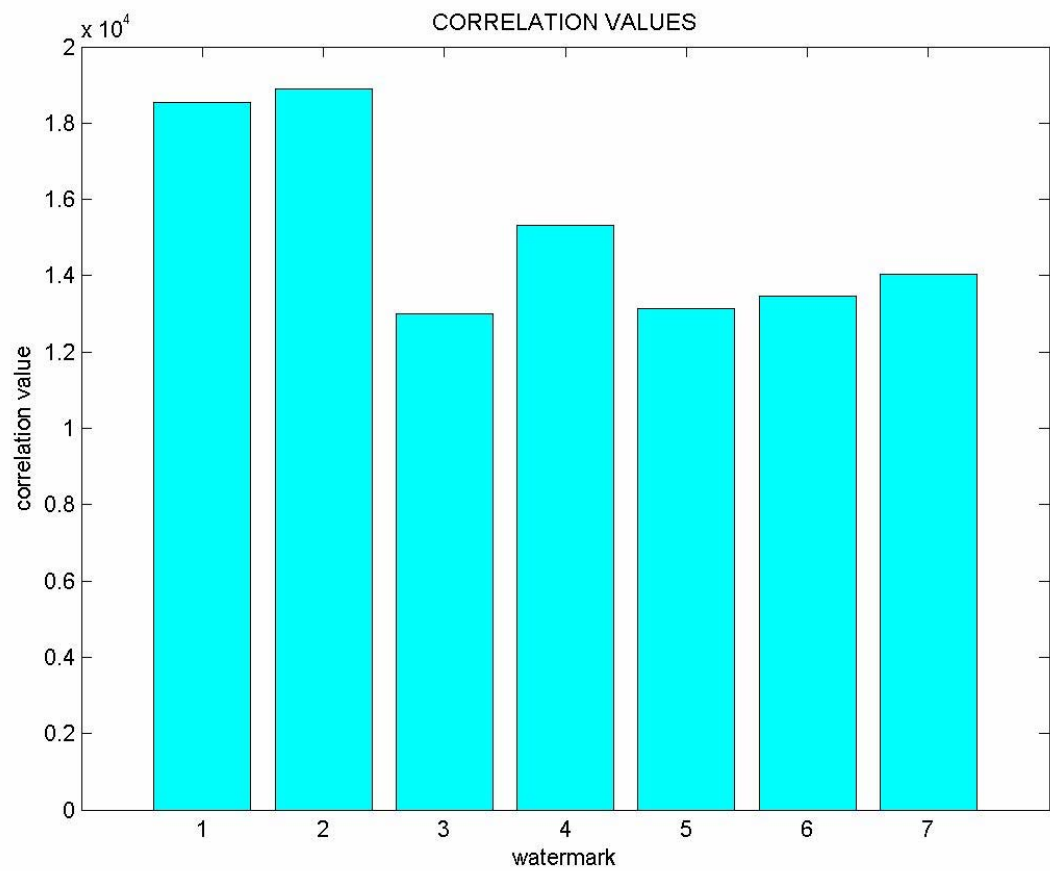
12. frame_dropped_video



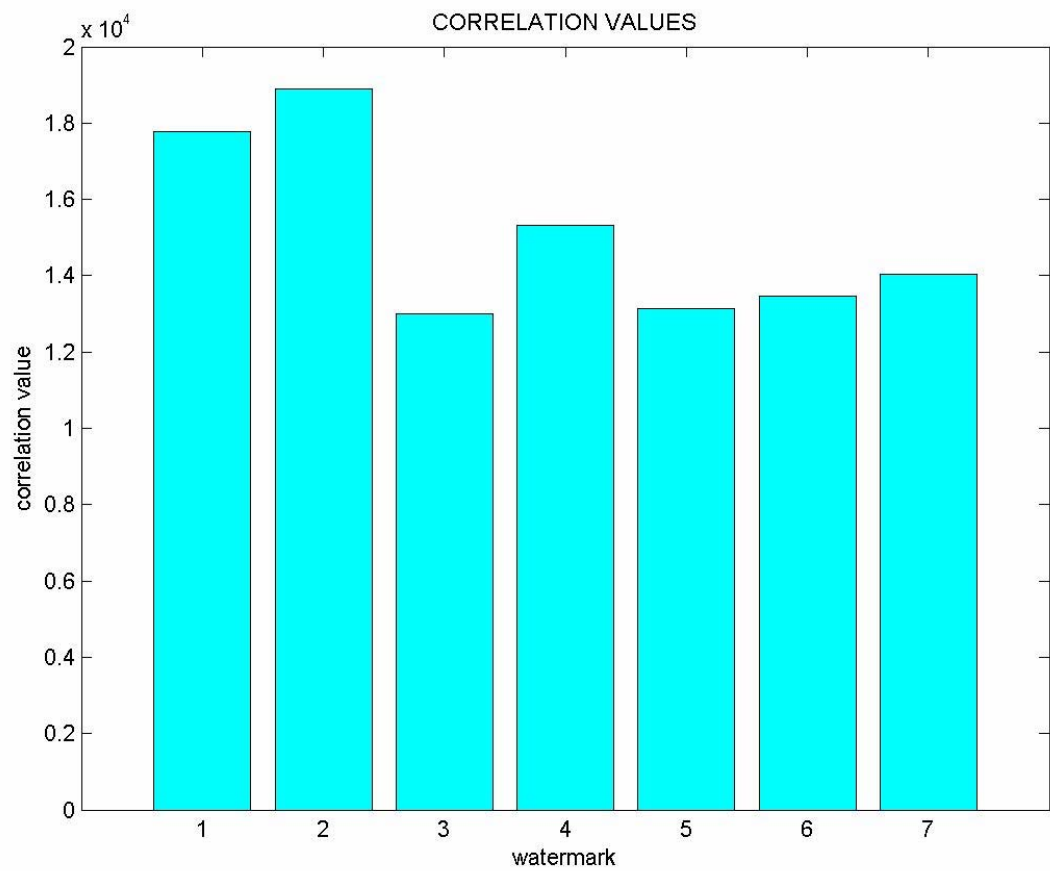
13. frame_swapped_video



14. frame_interpolated_video

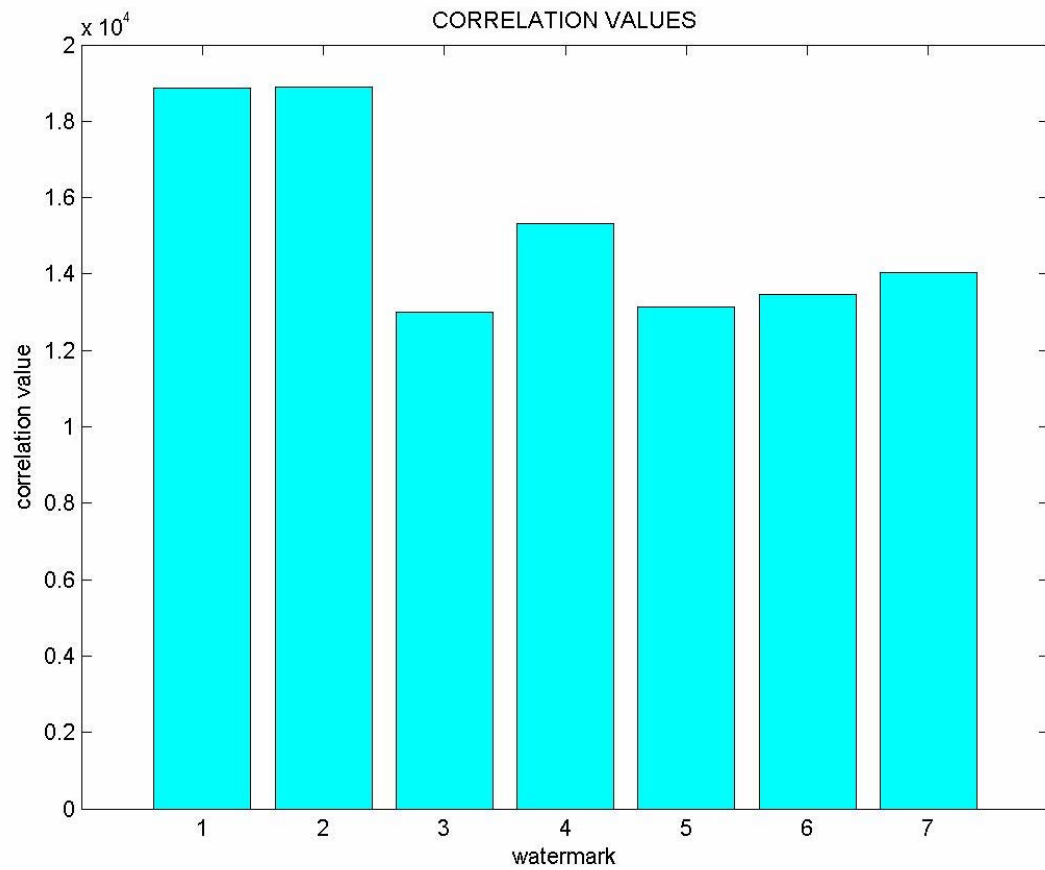


15. frame_resized_video

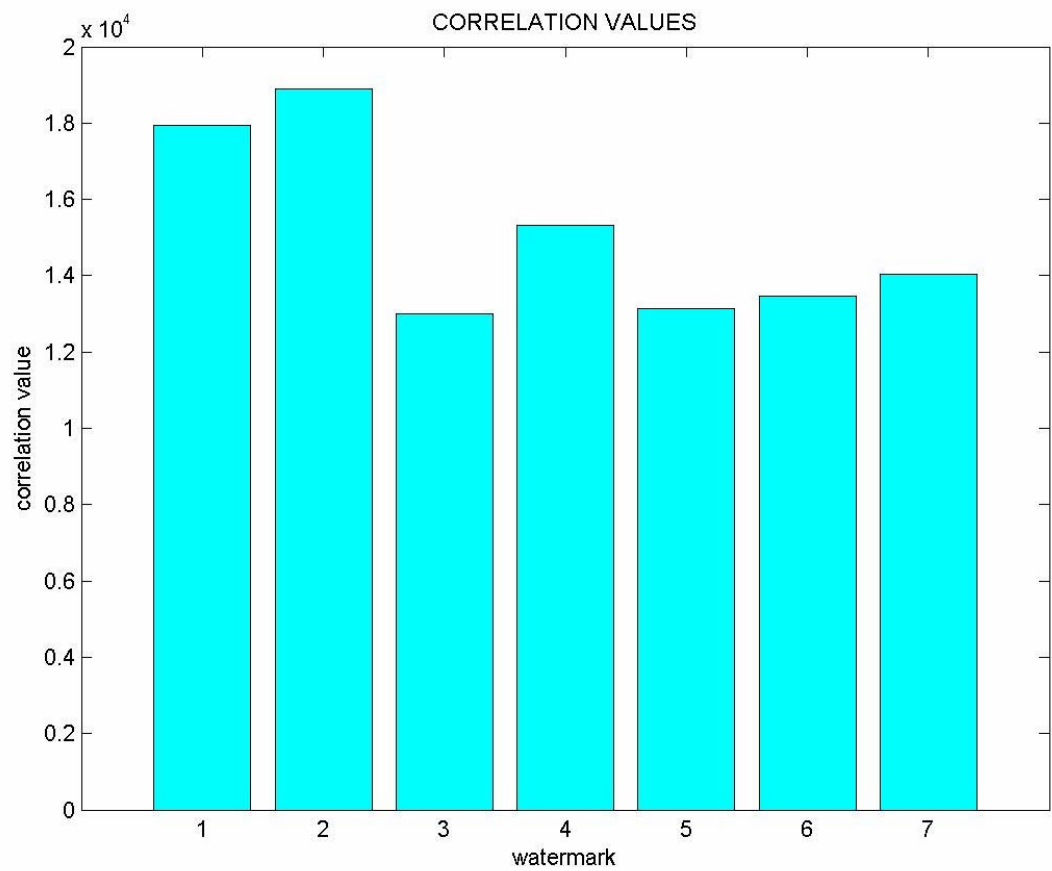


COMPARISON ON THE BASIS OF CORRELATION VALUES (WATERMARKING MID-SB PLANES)

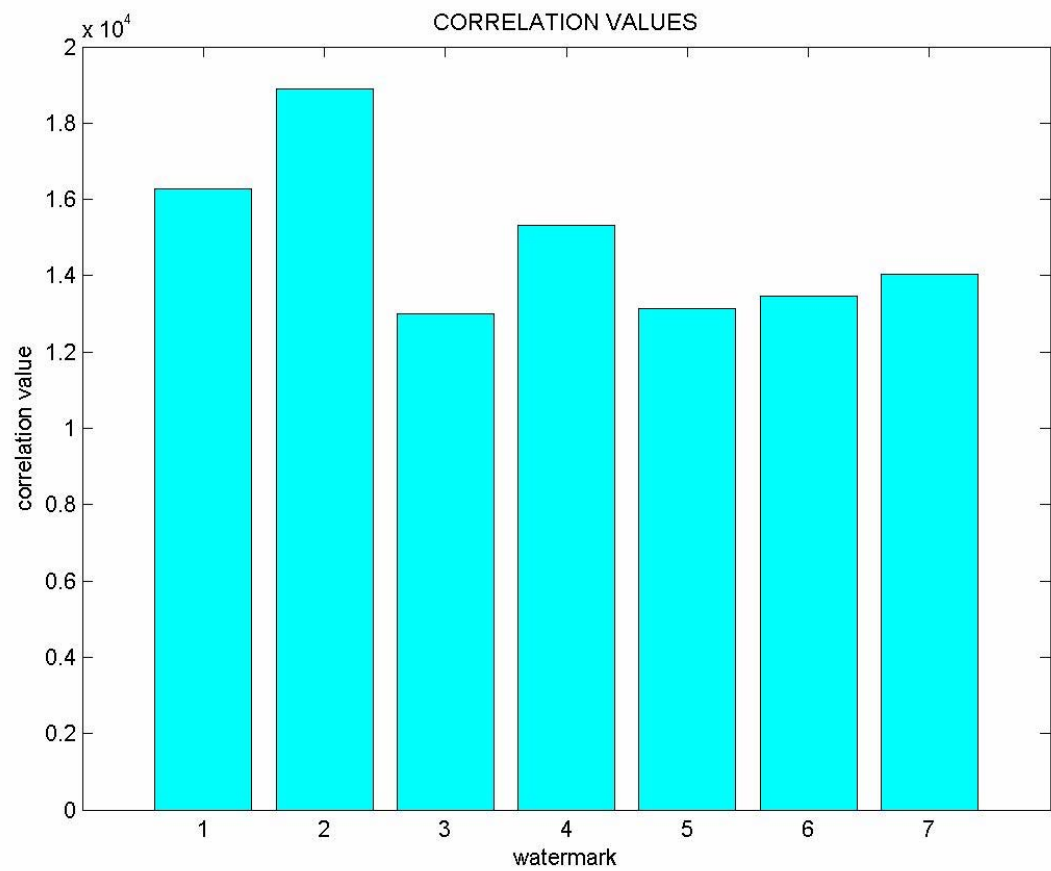
1. watermarked_video



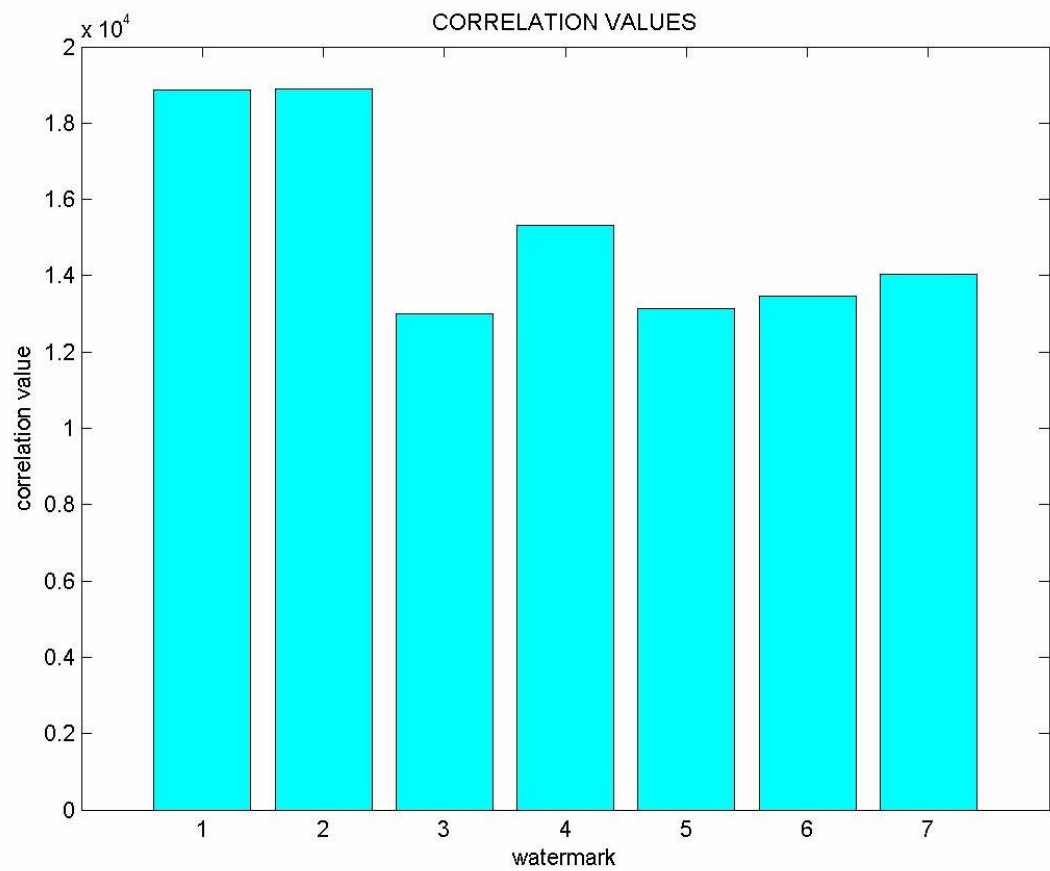
2. compressed_video



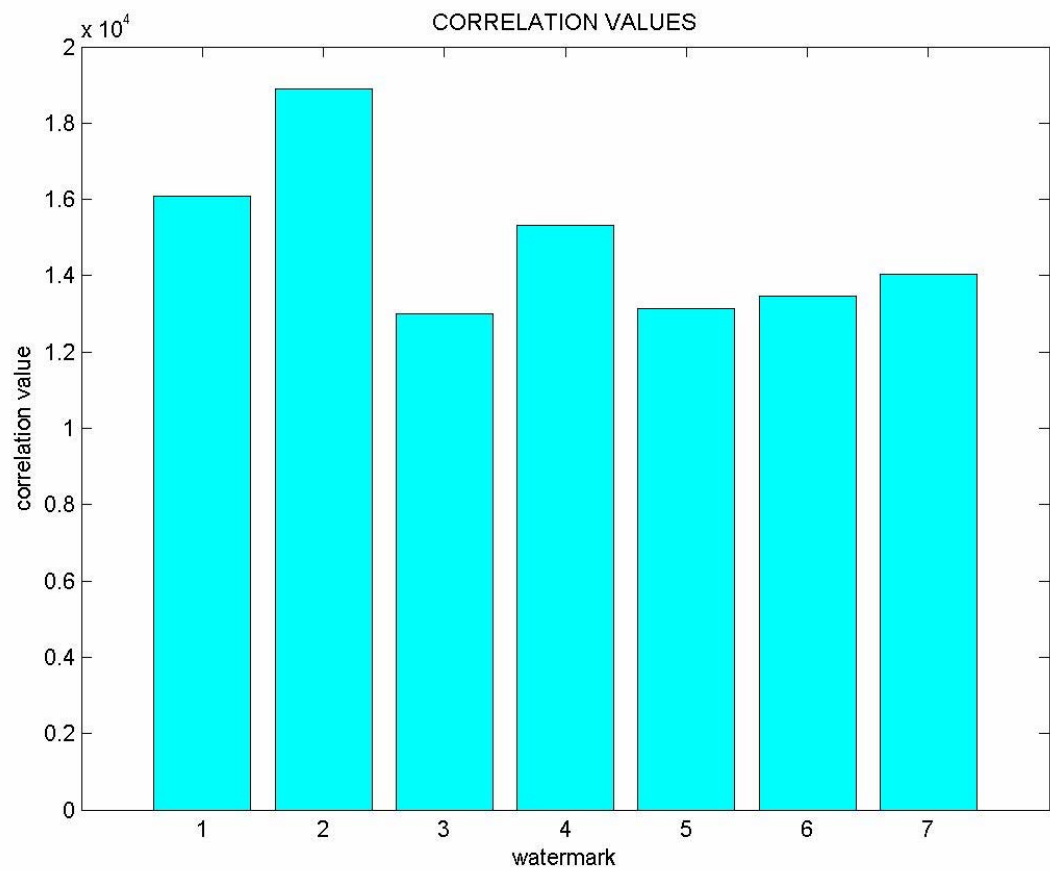
3. noisy_gaussian_video



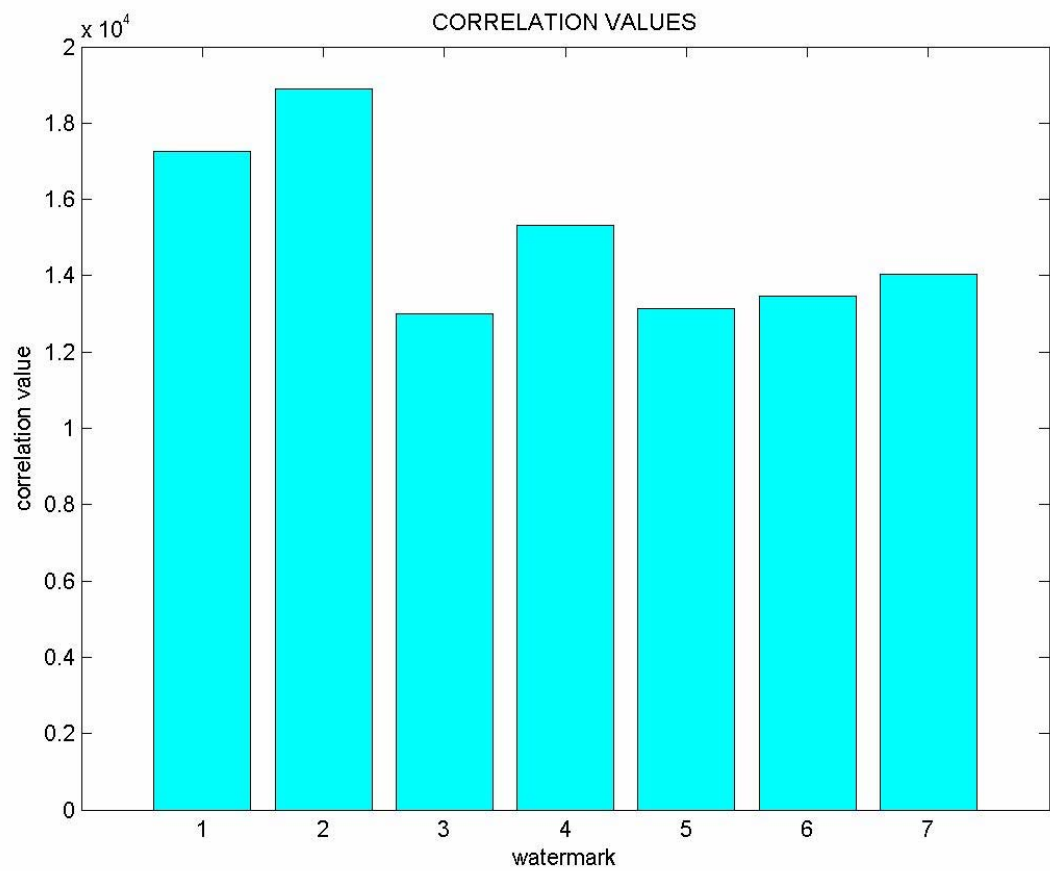
4. noisy_salt_pepper_video



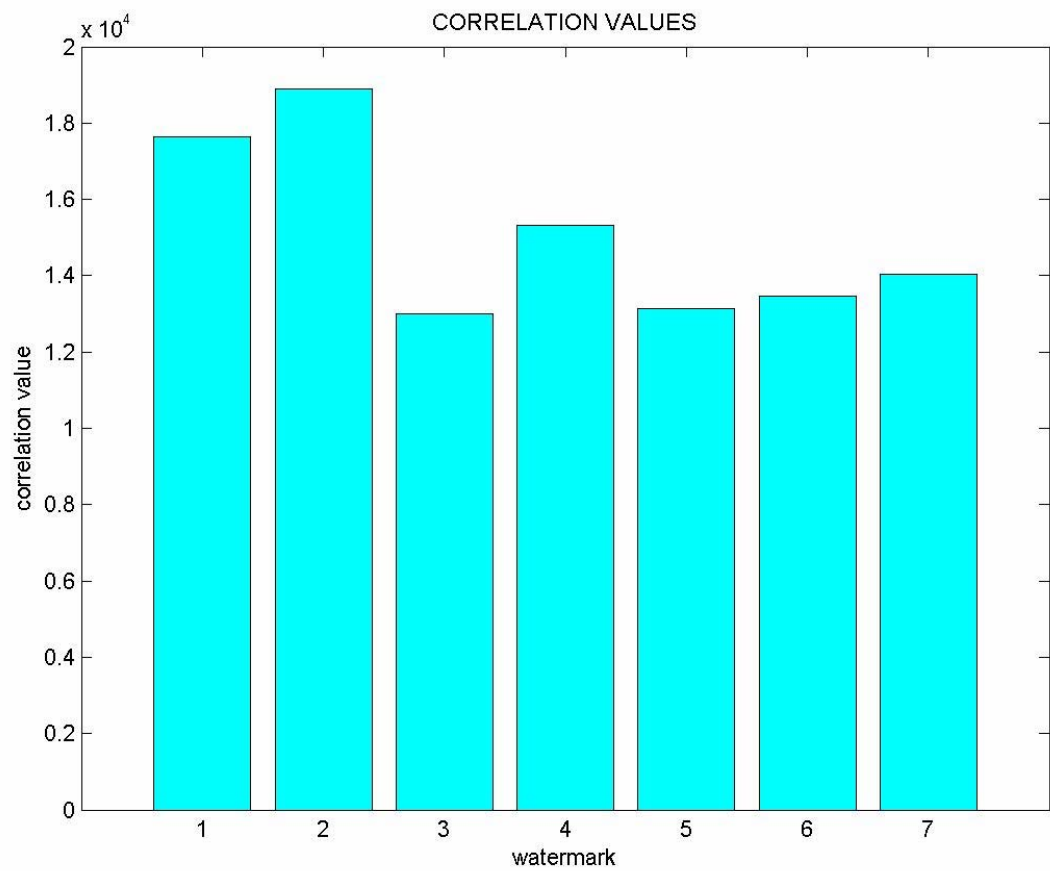
5. averaged_filtered_video



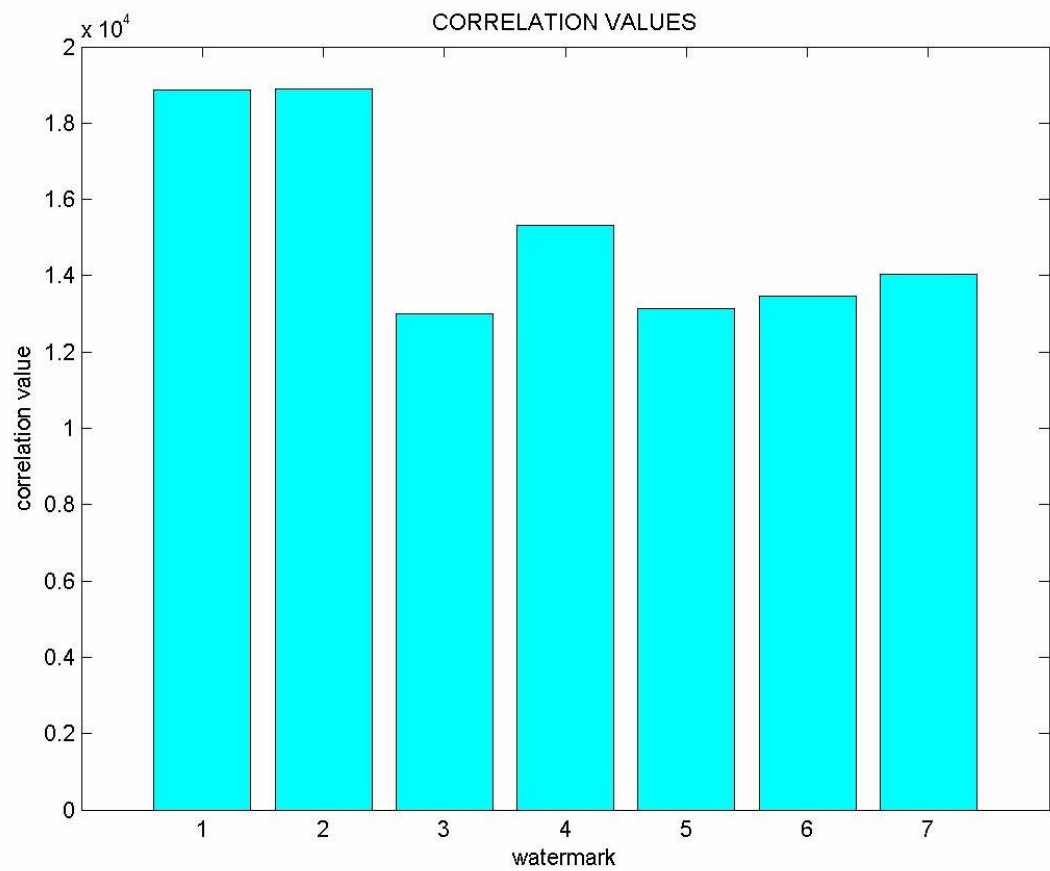
6. median_filtered_video



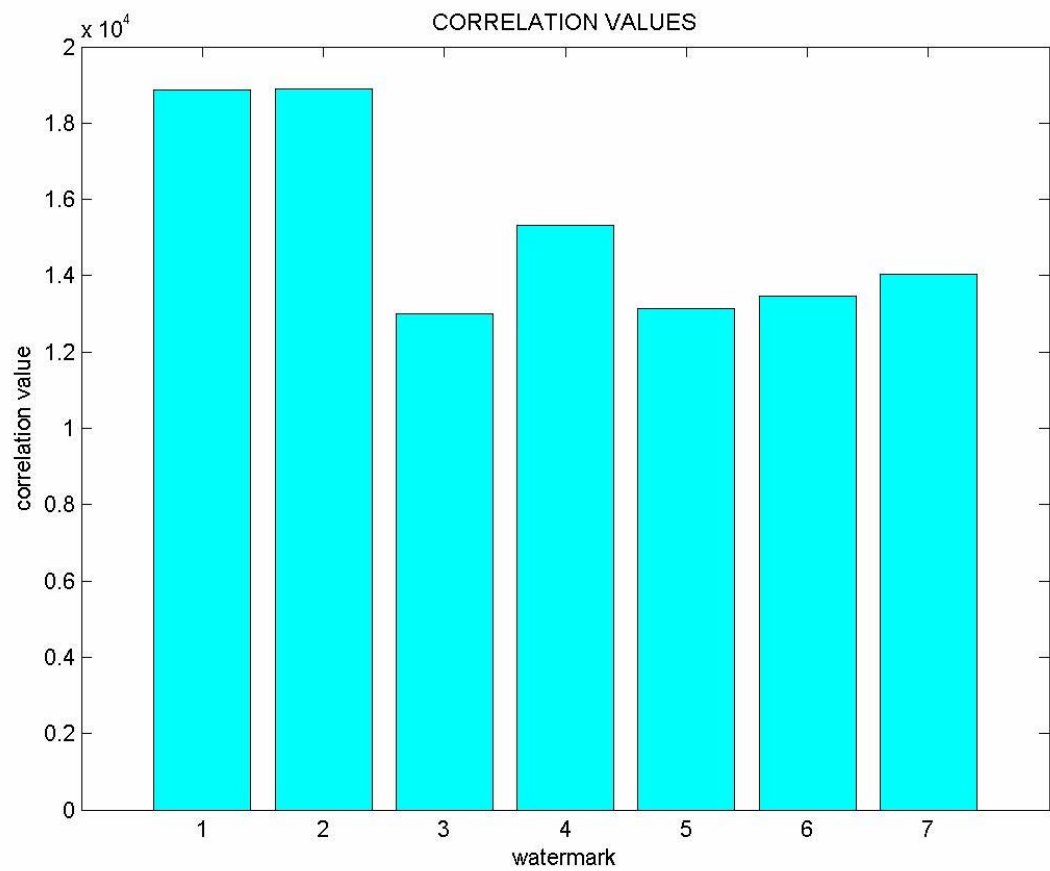
7. wiener_filtered_video



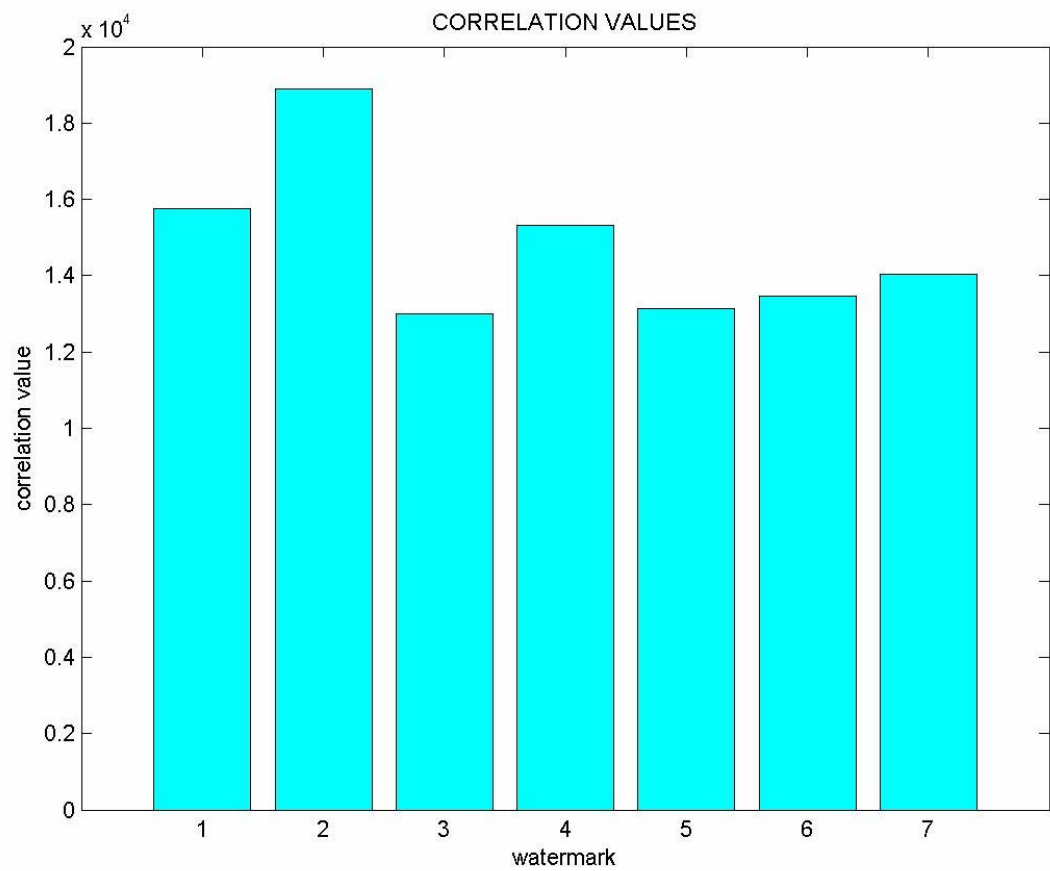
8. pixel_removed_video



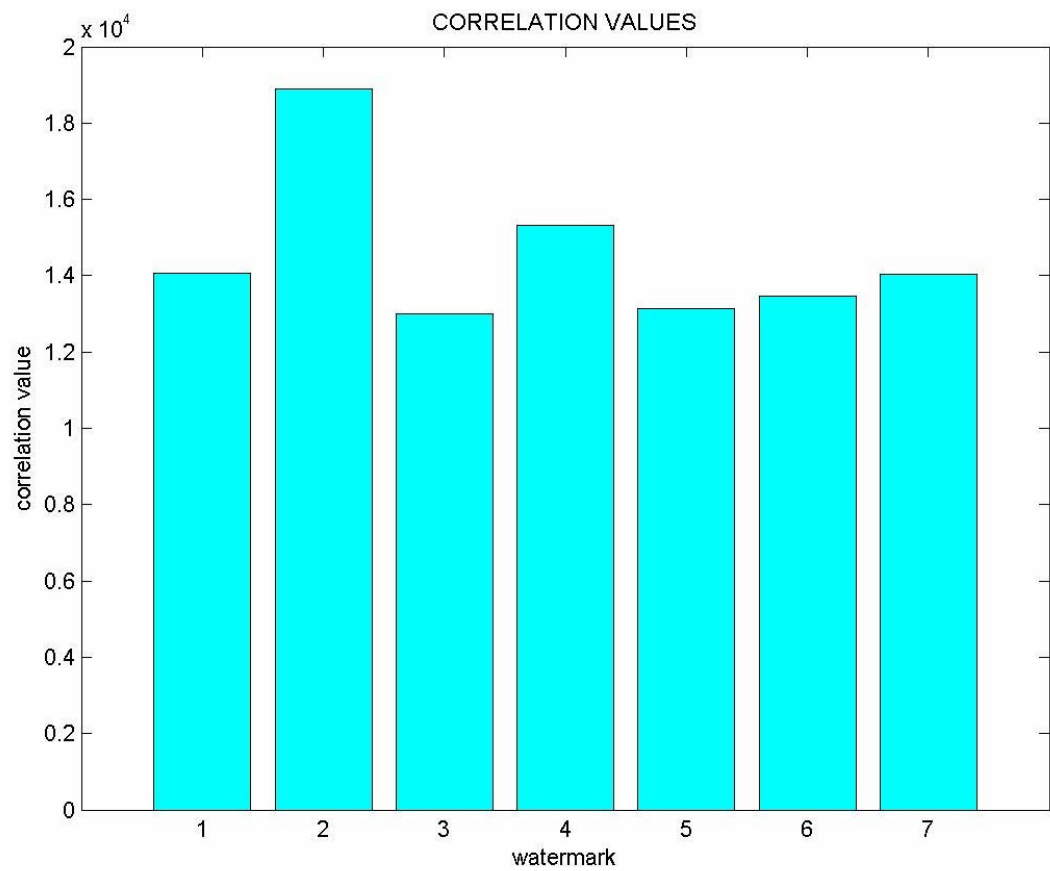
9. line_removed_video



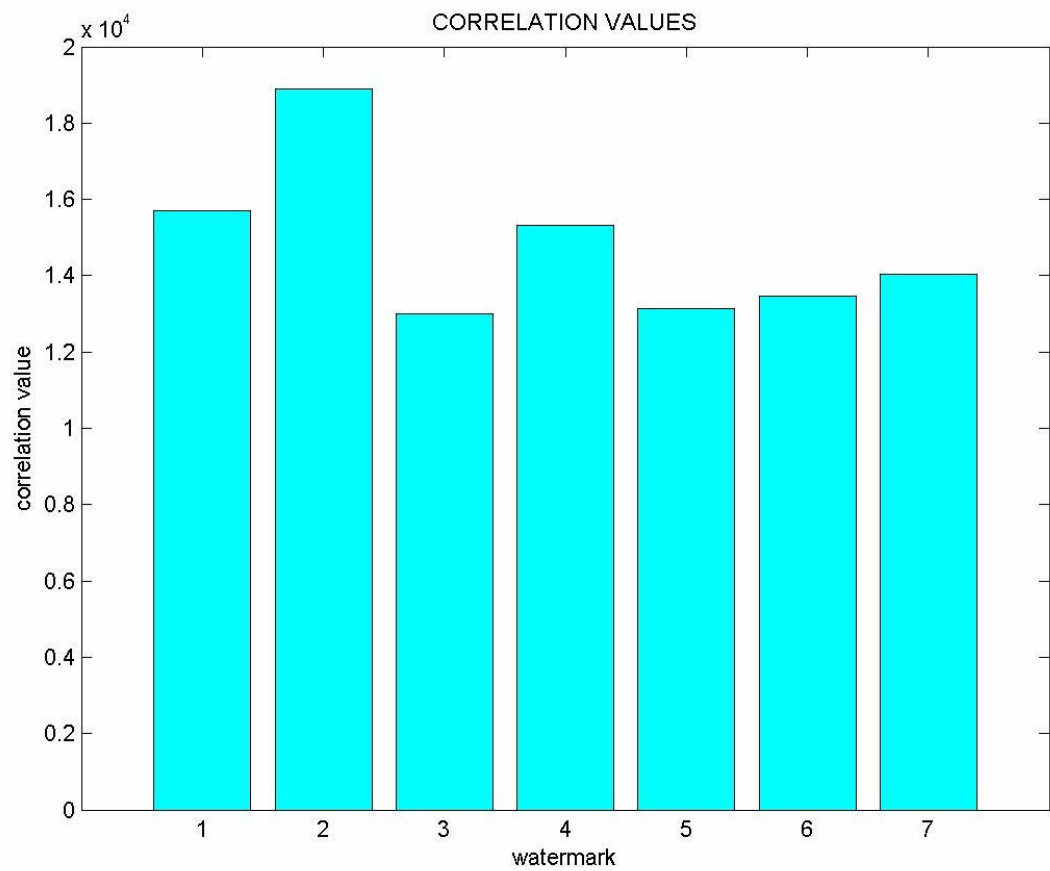
10. frame_removed_video



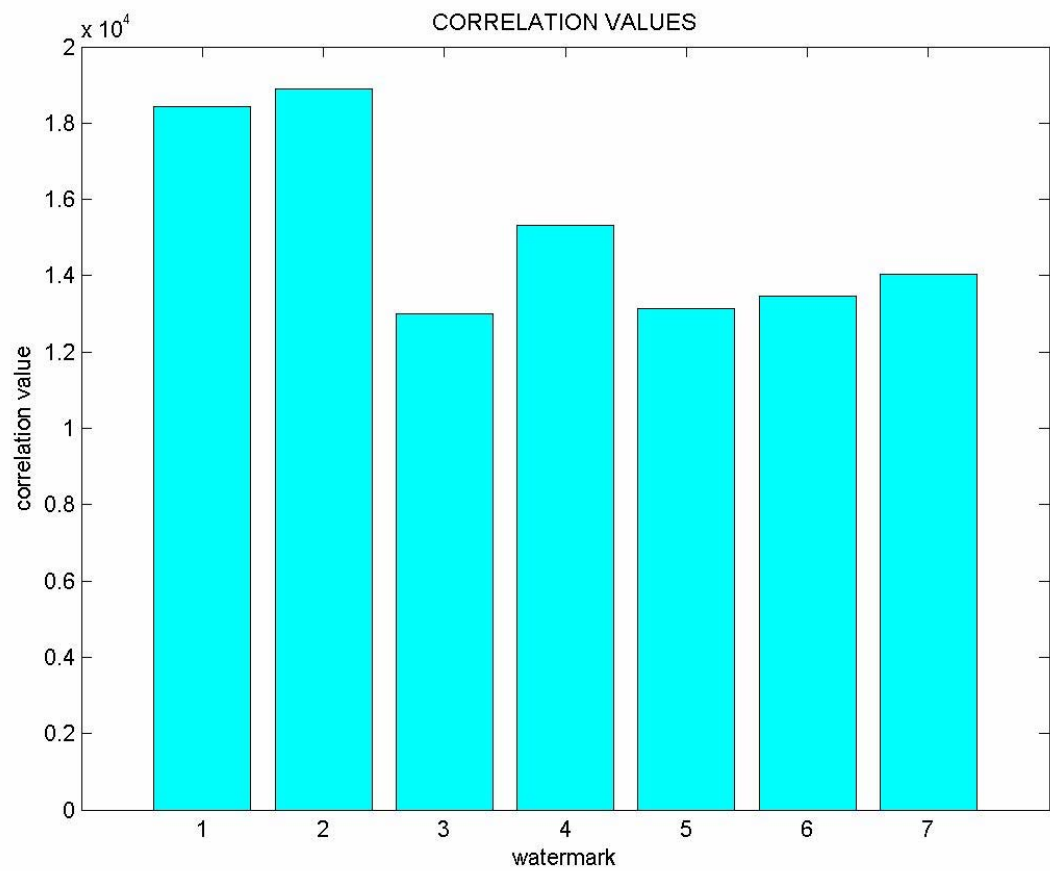
11. frame_rotated_video



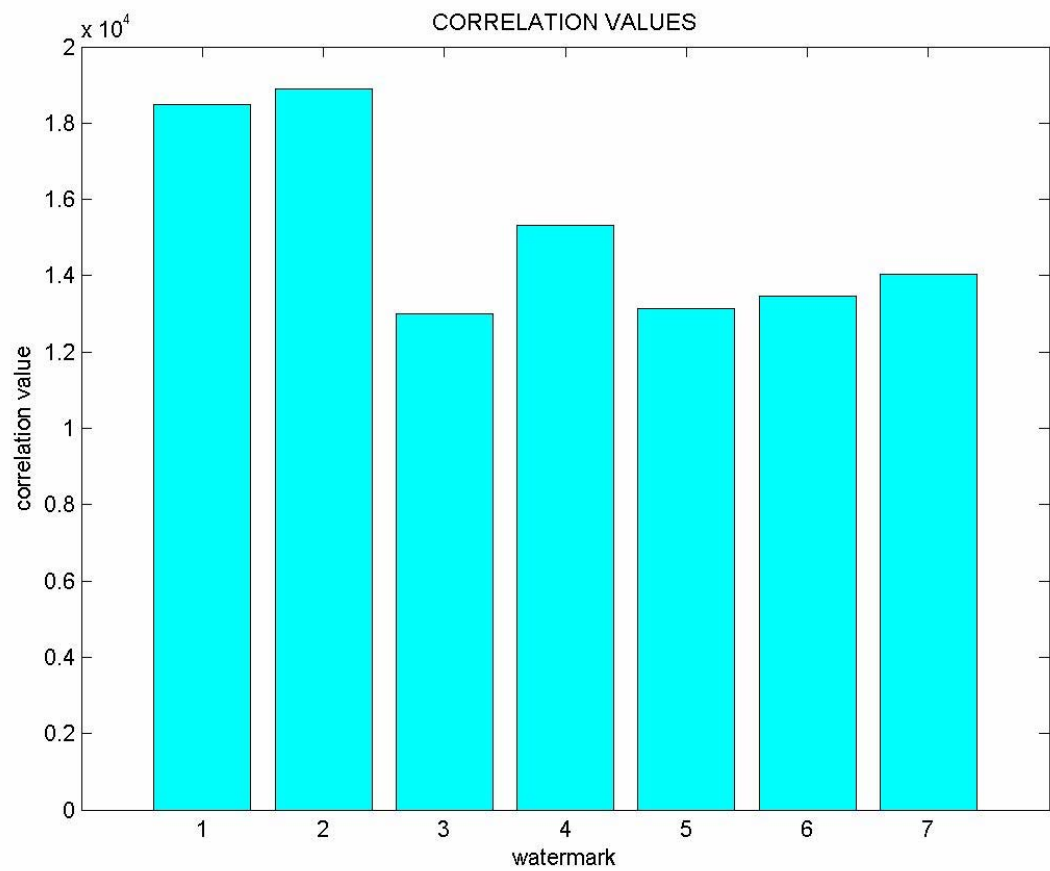
12. frame_dropped_video



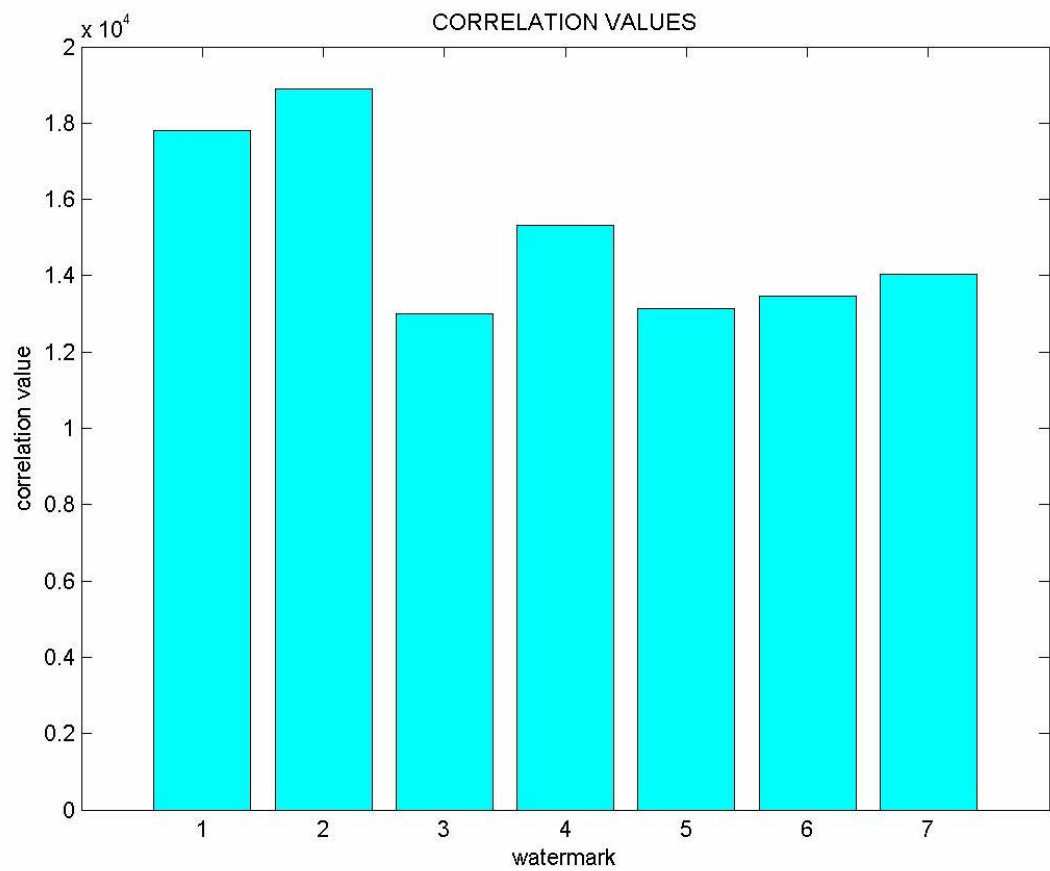
13. frame_swapped_video



14. frame_interpolated_video

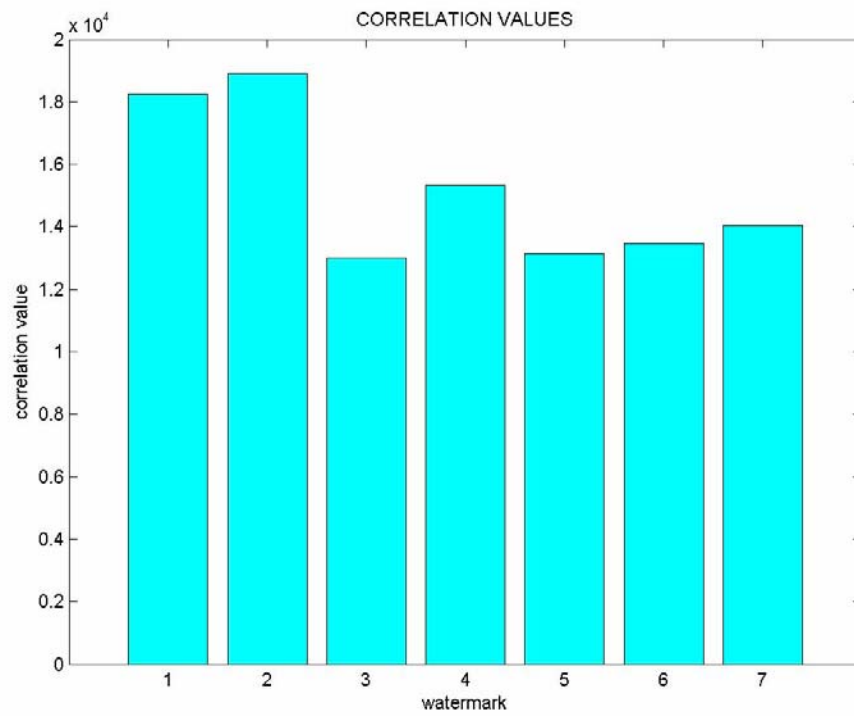


15. frame_resized_video

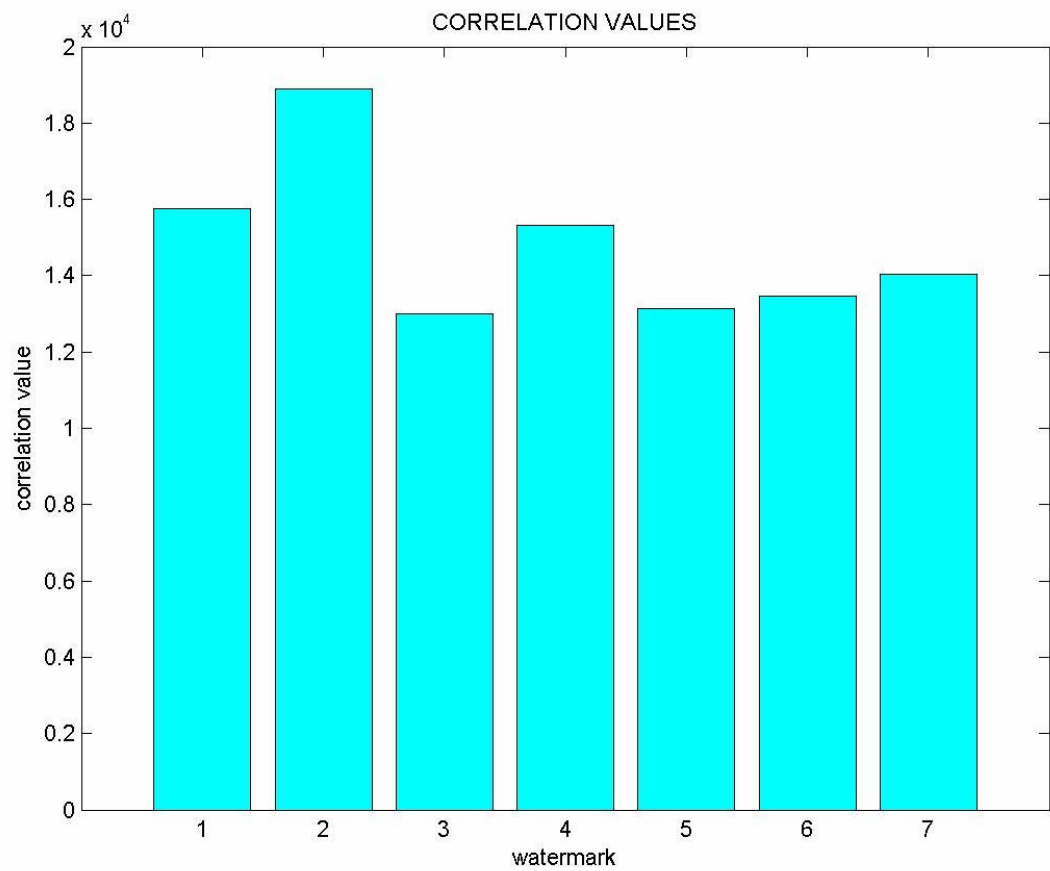


COMPARISON ON THE BASIS OF CORRELATION VALUES (WATERMARKING LSB PLANES)

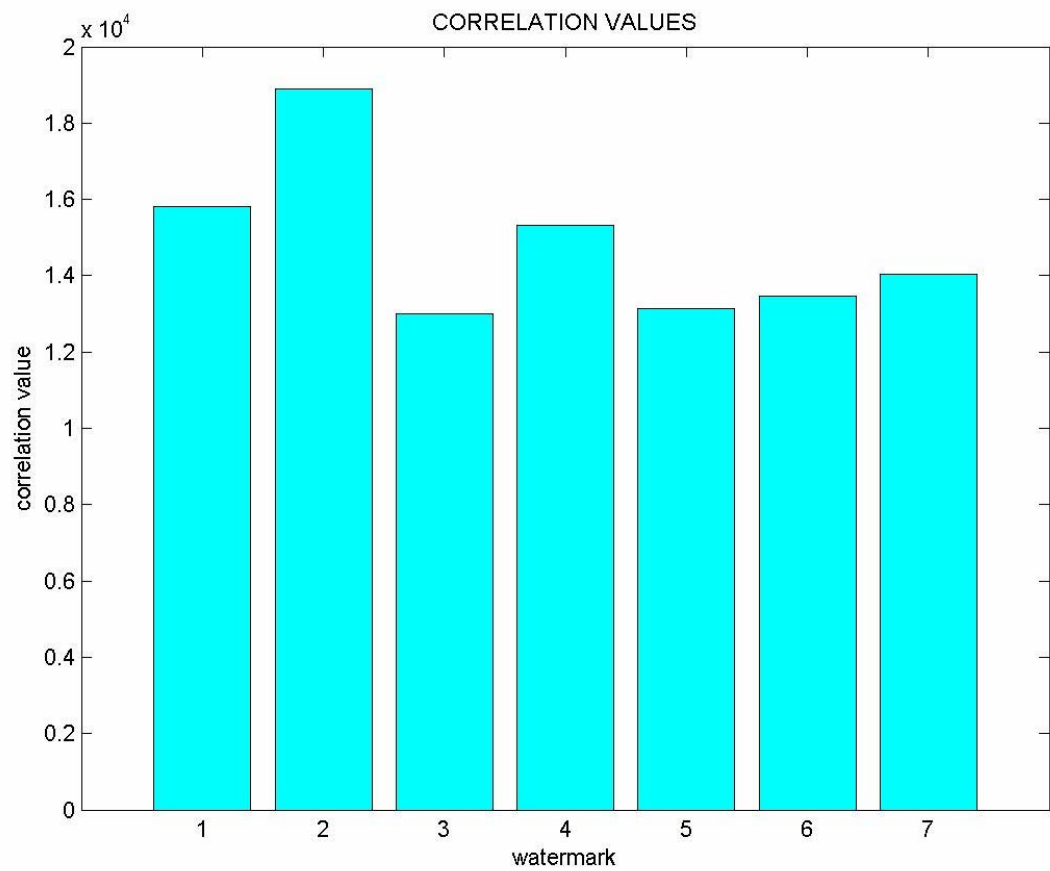
1. `watermarked_video`



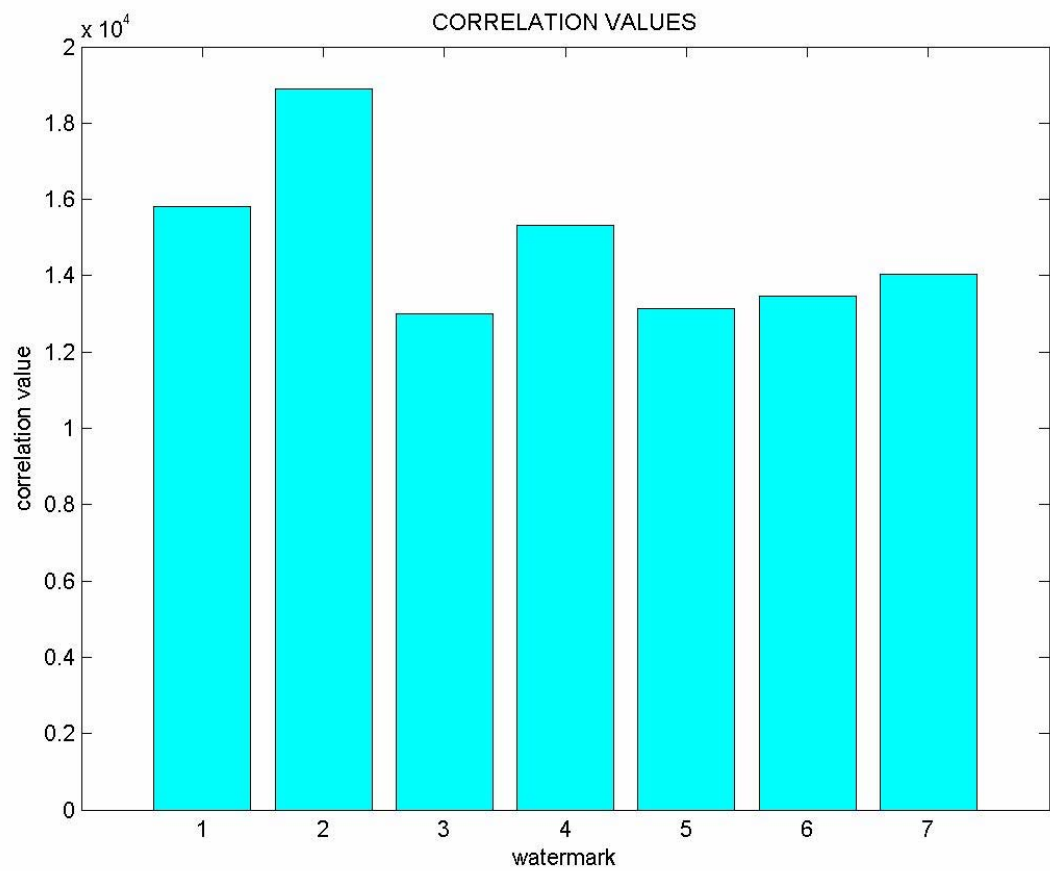
2. compressed_video



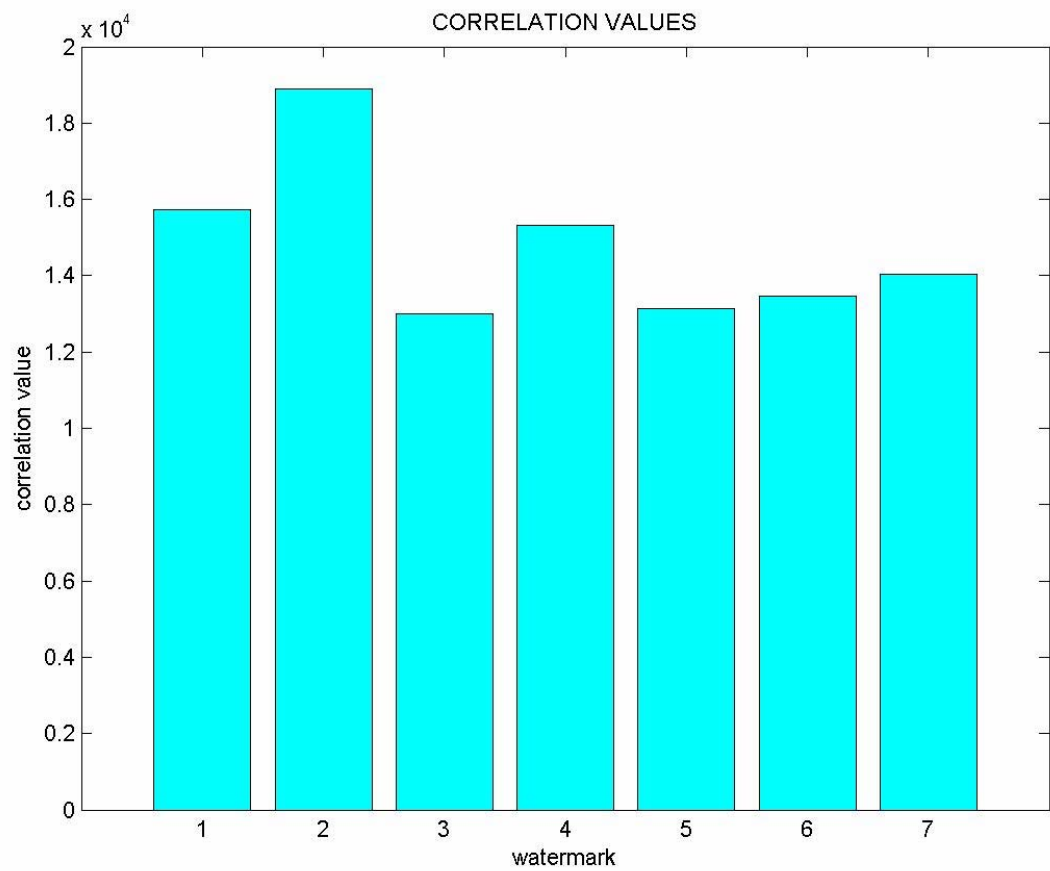
3. noisy_gaussian_video



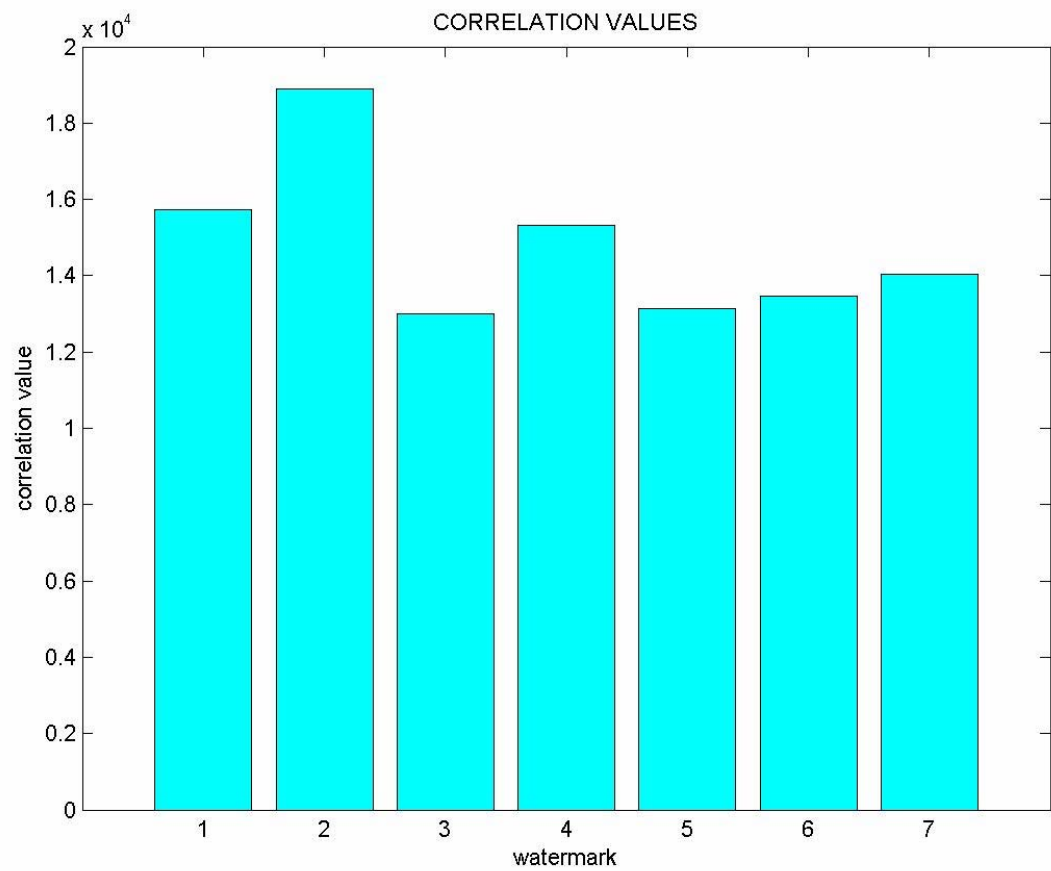
4. noisy_salt_pepper_video



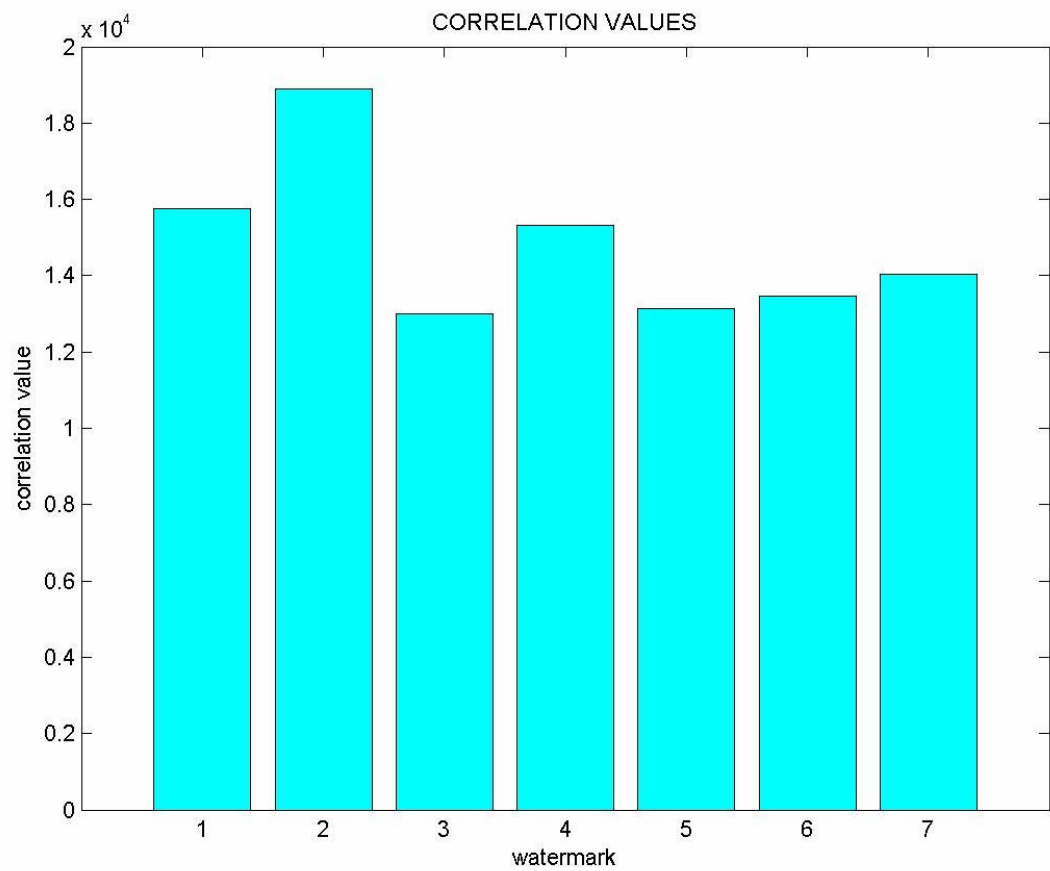
5. averaged_filtered_video



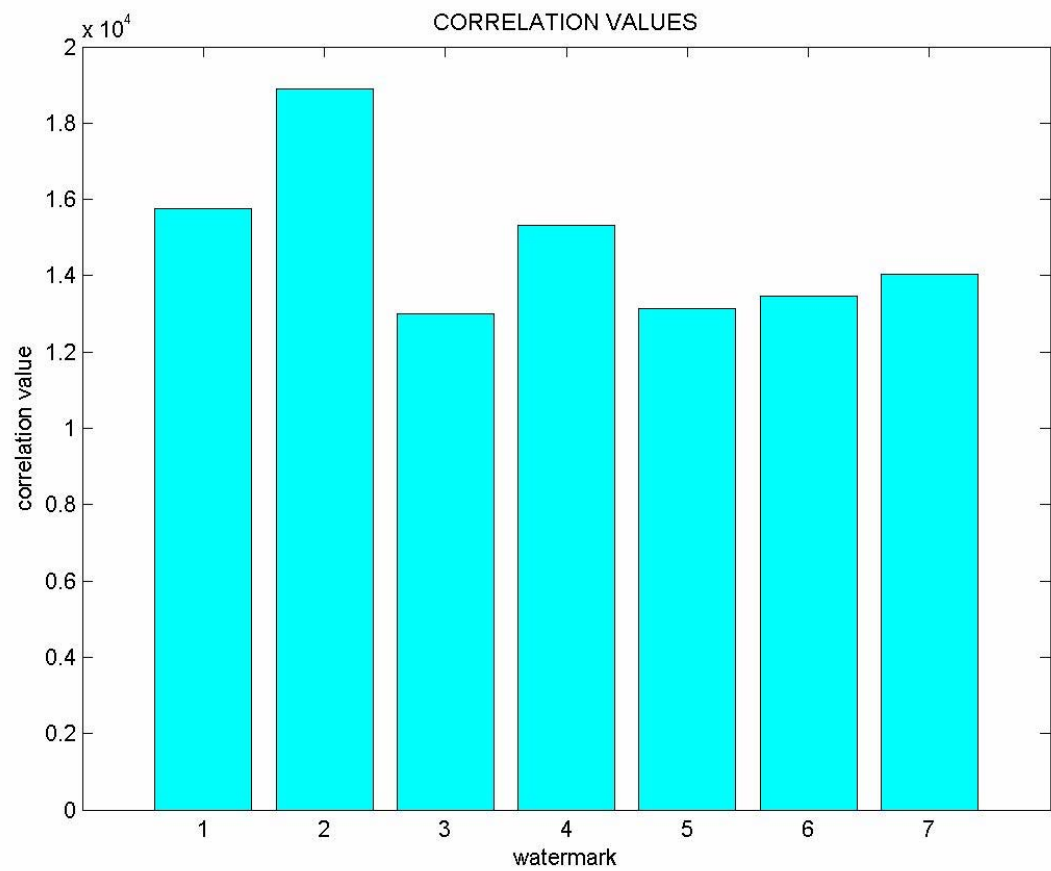
6. median_filtered_video



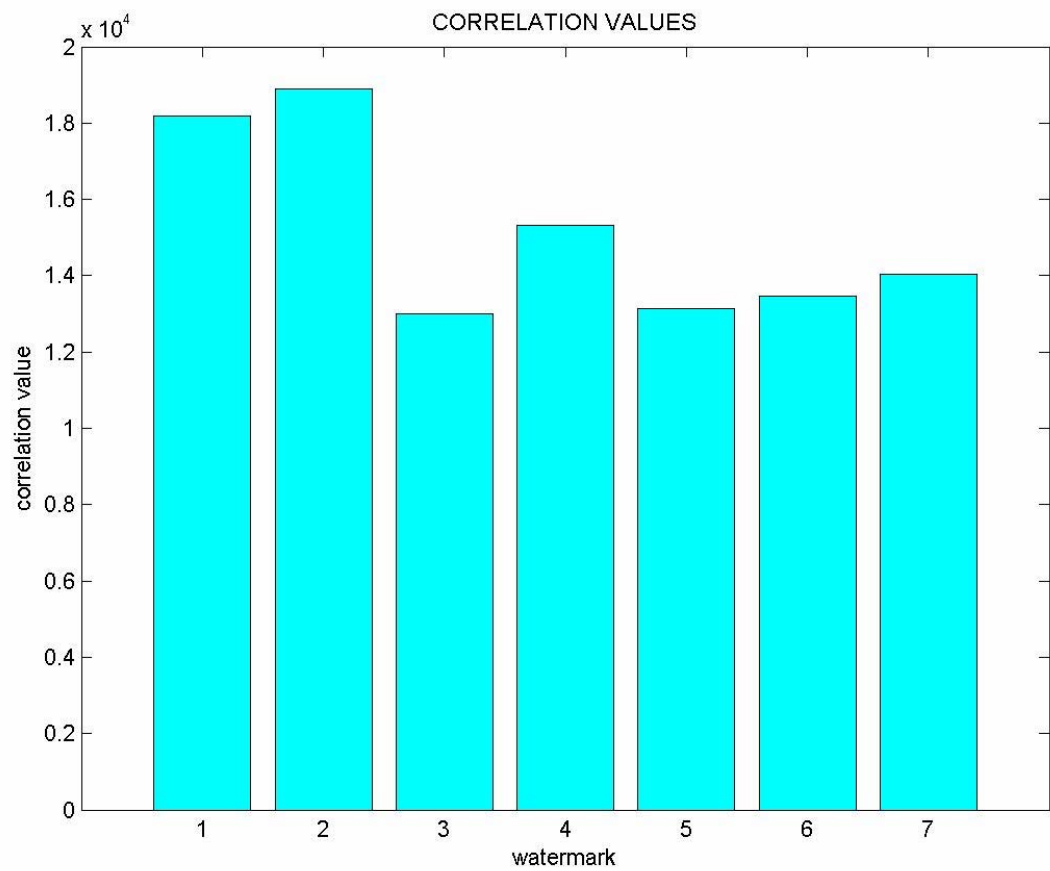
7. wiener_filtered_video



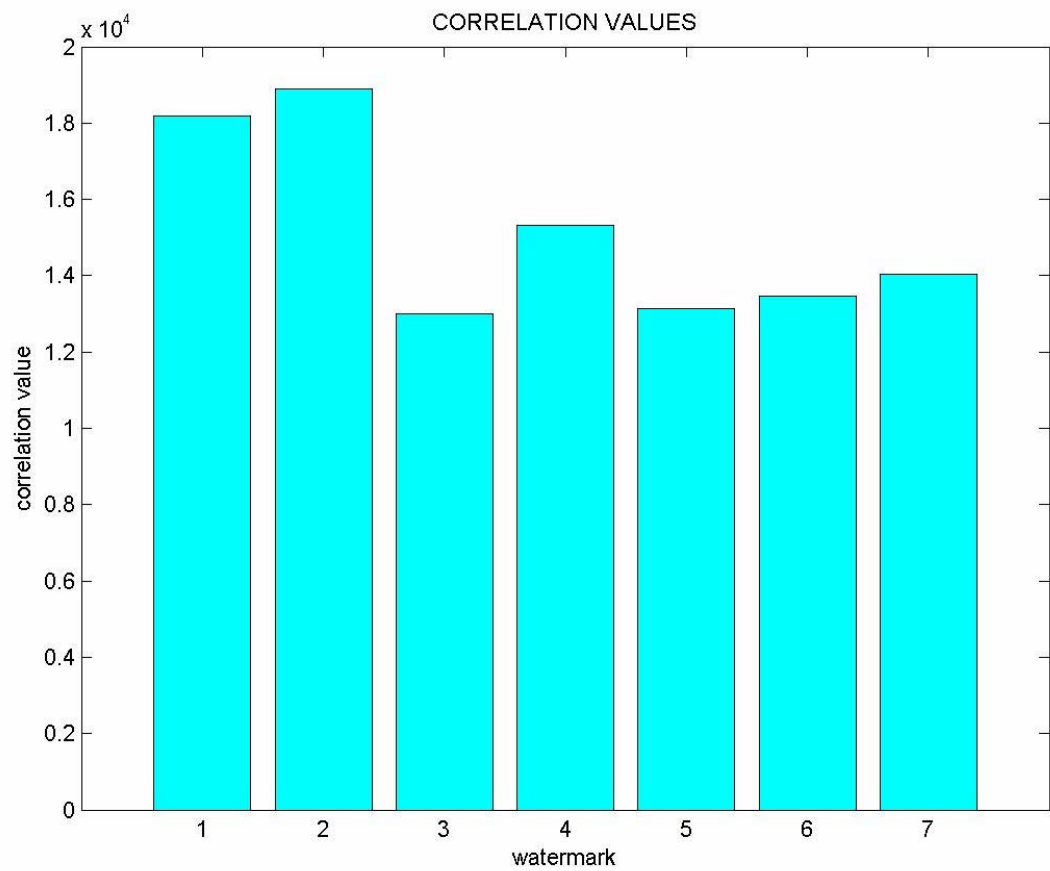
8. pixel_removed_video



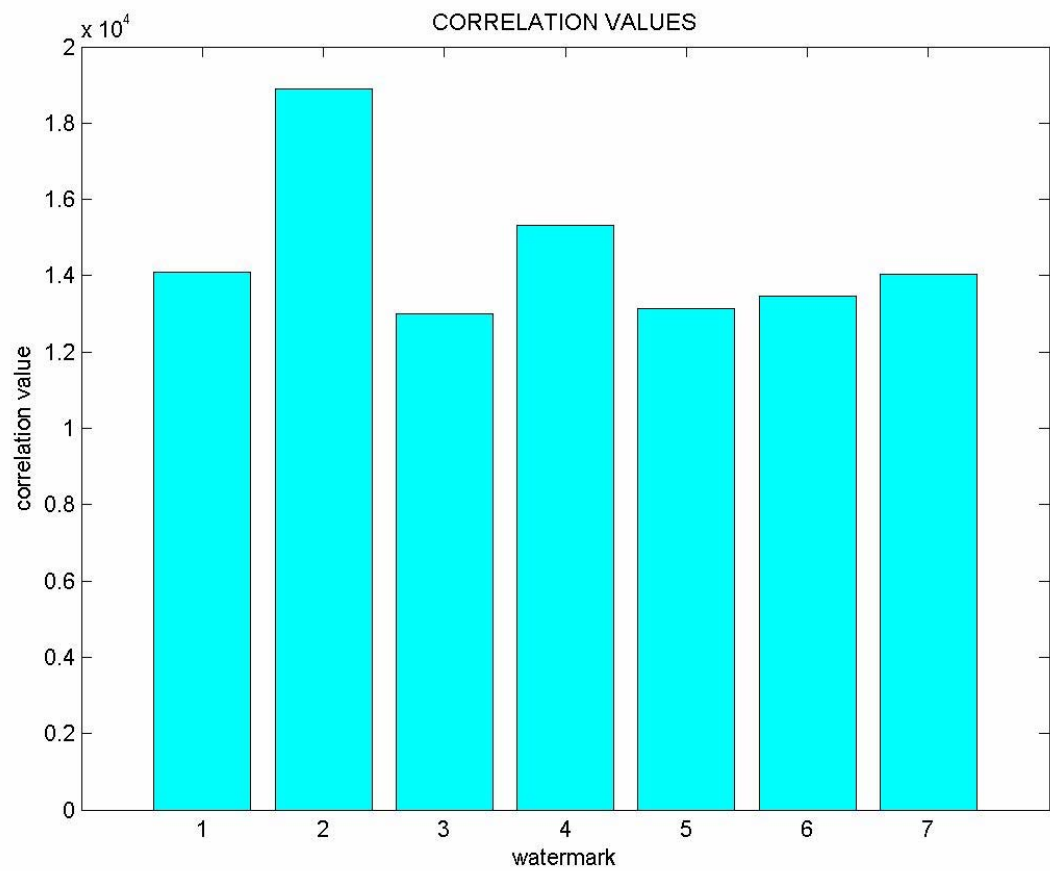
9. line_removed_video



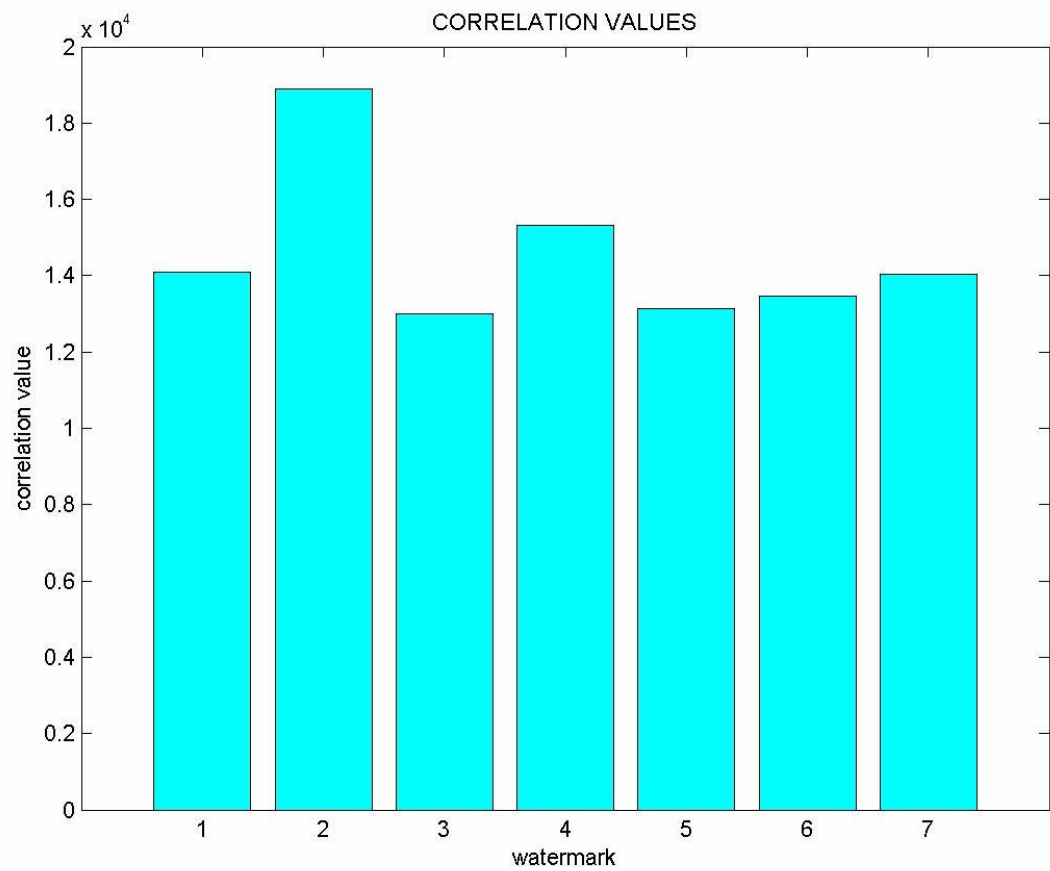
10. frame_removed_video



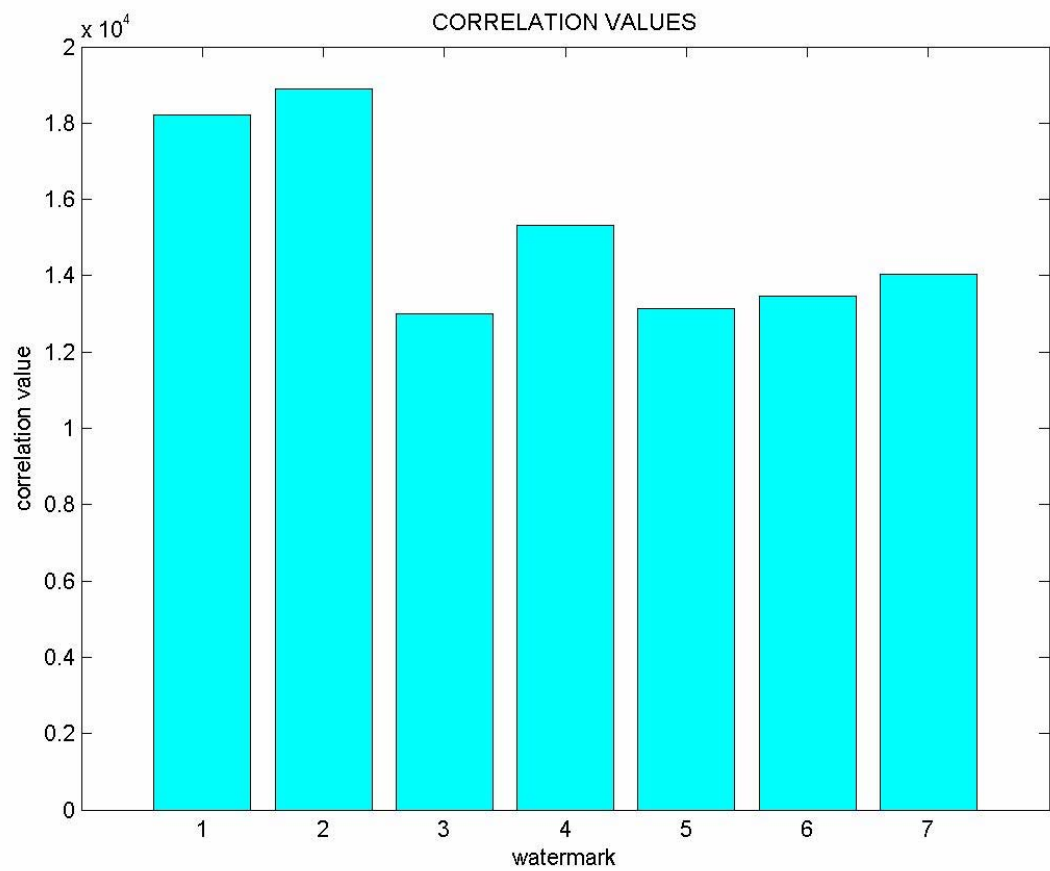
11. frame_rotated_video



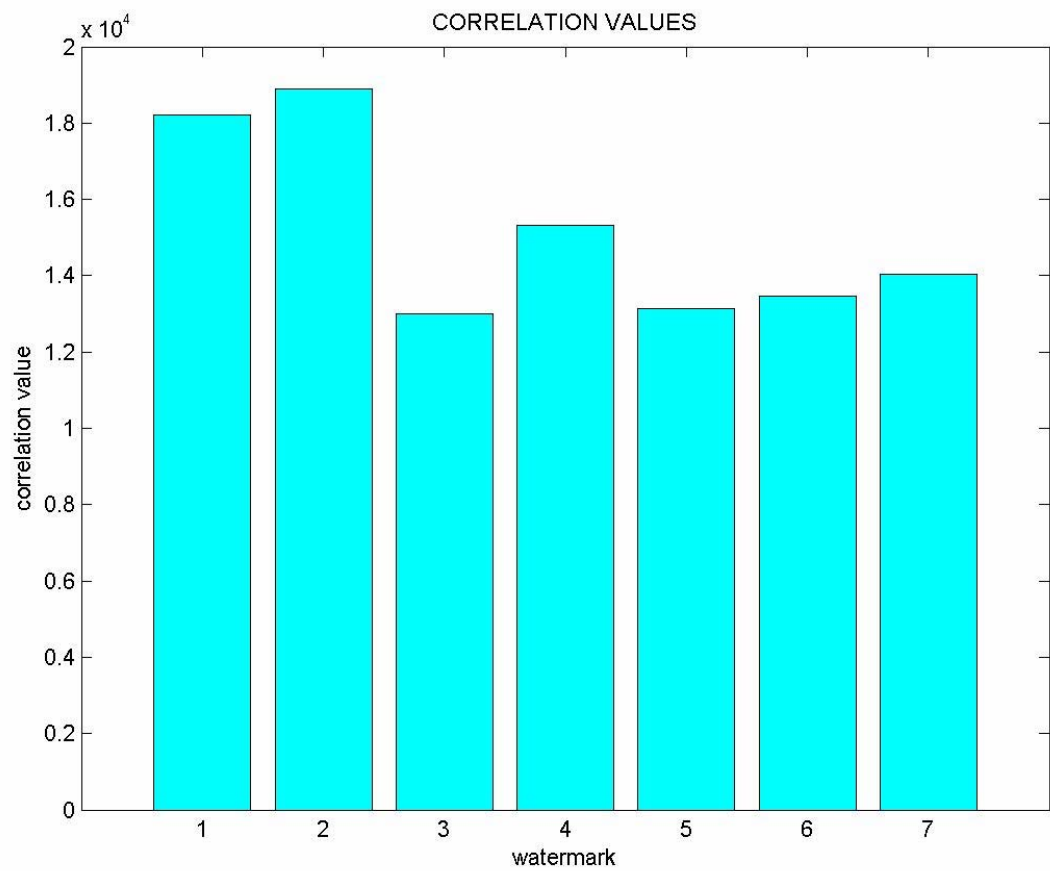
12. frame_dropped_video



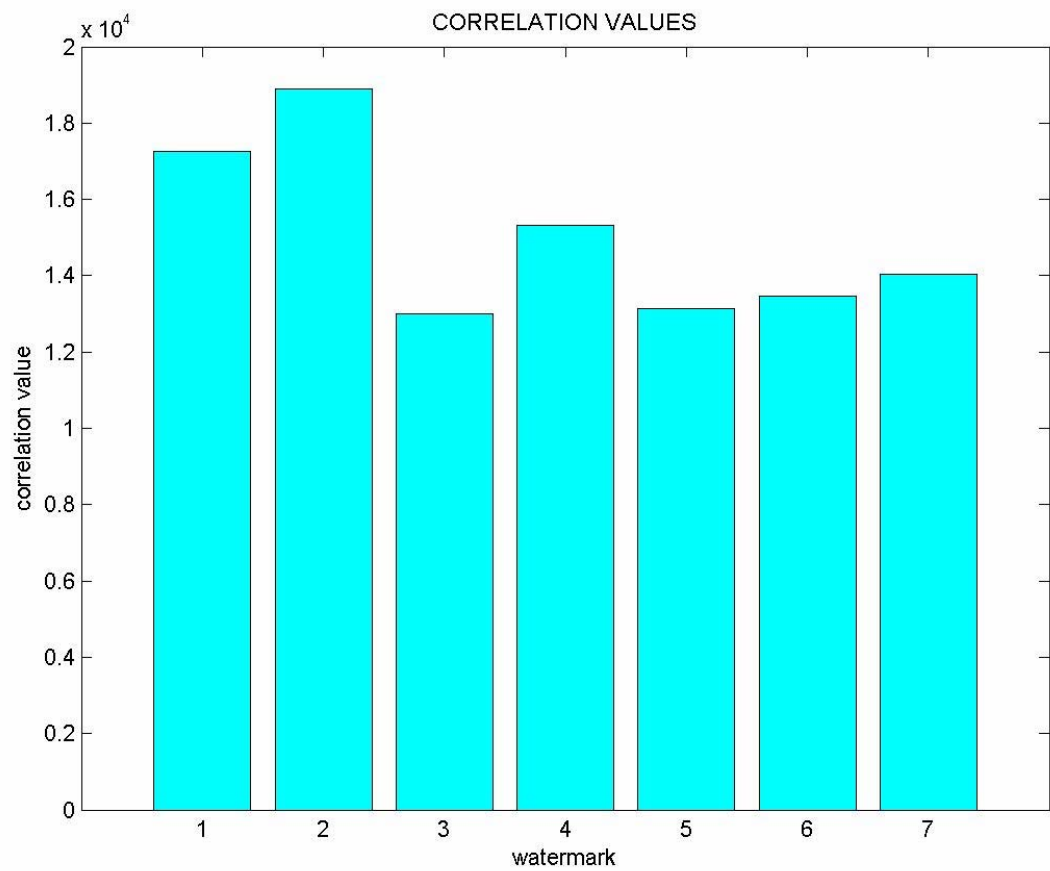
13. frame_swapped_video



14. frame_interpolated_video



15. frame_resized_video



PROJECT IMPLICATIONS --:

- ❖ Would help students of the college develop interest in the field of spread spectrum techniques and its use for digital Image and Video Watermarking.
- ❖ Would help them visualize through appropriate waveforms how system response varies with variations in parameters like chip-rate etc.
- ❖ Could prove to be an effective tool to study effect of various types of attack on a Watermarking System and hence aid in designing an optimum system .

FUTURE OF THE PROJECT --:

- ❖ Using other techniques instead of DSSS for Watermarking.
- ❖ Working in the Frequency domain instead of Spatial-Domain for the obvious reasons.
- ❖ Working on Compressed Video for Watermarking instead of the Raw Video.
- ❖ Using newly developed Motion estimation technique for Digital Video Watermarking.

LIST OF TABLES

Tab 1.1 COMPARISON TABLE (WATERMARKING MSB PLANES)

Tab 1.2 COMPARISON TABLE (WATERMARKING MID-SB PLANES)

Tab 1.3 COMPARISON TABLE (WATERMARKING LSB PLANES)

LIST OF FIGURES

Figure 2.1	Digital Watermarking
Figure 2.2	Visibility problem in consecutive frames(A)
Figure 2.3	Visibility problem in consecutive frames(B)
Figure 2.4	Graphical representation of CDMA digital Video Watermarking
Figure 3.1	Modulator
Figure 3.2	Building blocks of a DSSS system for BPSK Modulation
Figure 3.3	Spread –spectrum technique
Figure 3.4	De-spreading technique
Figure 5.1	Watermarking Model
Figure 5.2	Video Modeled as a stream of bit planes
Figure 5.3	Complete Model of the digital Video watermarking
Figure 5.4	Direct Sequence Spread Spectrum Module
Figure 5.5	Working of the Stage I
Figure 5.6	Model of the Stage II (Attacking Stage)
Figure 5.7	Model of the Stage III (Watermark Detection Stage)
Figure 5.8	Model of the De-Spreading Module
Figure 5.9	Working of the Stage III (Watermark Detection Stage)

GLOSSARY

IMAGE CRYPTOGRAPHY

Image cryptography is considered as an encoding technique for data transmission through communication channels under condition that a third party could not read and interpret the data [80]. However, transmitted data, especially in scrambled form, can attract attention and impel law-enforcing authorities to take a closer look [41]. Nevertheless, cryptography has become one of the main tool for privacy, access control, authentication, digital signatures and secure messaging.

Steganography implants the secret message in some form of cover data, typically digital images or video streams, concealed as 'noise'. Without the correct key, it is virtually impossible to extract the hidden message or even detect its presence. This places an additional burden on the cryptanalyst who now has to examine unsuspecting-looking data for embedded steganographic messages [68].

Steganographic messages are usually encrypted in order to increase security, but also to conceal any statistical significant patterns. For image-type messages, mixing systems based on toral automorphisms [247, 248] or Kolmogorov flows [206] can be used.

The second relationship between cryptography and watermarking stems from the shared semantics of public- and private-key crypto-systems versus public- and private-key watermarking systems. In private-key crypto-systems, the same key is used to encrypt and decrypt a message (symmetric cipher), while in public-key crypto-systems, the keys for encryption and decryption are different (asymmetric cipher).

PUBLIC – KEY WATERMARKING

In a public-key watermarking system, a digital object is marked with the private key but the presence of a watermark can be checked using a public key. Of course, computation of the corresponding private key is infeasible, despite the availability of the public key and the algorithm of the watermarking system. The public key only allows to read the watermark, it can not be used to remove or forge a watermark. Public-key watermarking generally assumes that the unmarked original host is not required in the detection or extraction process (blind recovery).

Traditional watermarking systems using symmetric, private keys almost always allow to remove or insert forged watermarks. Public-key schemes have to permit secure watermark verification by third persons. However, no public-key watermarking schemes is known to exist, since most current approaches can not withstand public detector device attacks as described by Kalker and Linnartz [98, 140].

ASYMMETRIC WATERMARKING

Asymmetric watermarking techniques do not refer to the original image and employ different parameters than the ones used in the embedding process. The terms public-key watermarking and asymmetric watermarking are often used in the same context. If you take the terms literally you might differ between asymmetric watermarking, the keys enabling watermark detection differ from the keys needed for embedding the watermark, and public-key watermarking, the keys necessary for watermark detection are publicly known, thus, enabling everybody – including potential attackers – to detect an embedded watermark. Asymmetric watermarking might actually be a way of realizing a public-key watermarking system.

The public detector device attack described by Kalker and Linnartz [98, 140] which is based on the linearity of the detection process, does not work on asymmetric schemes, e.g. see Eggers [64, 62].

VISUAL CRYPTOGRAPHY

Visual cryptography is a type of a cryptographic scheme to conceal images without any cryptographic computations. It is a visual variant of the k out of n secret sharing problem. One would produce transparencies that contain parts of the secret. Any k of the n transparencies stacked on a heap would reveal the secret, but less than k transparencies do not reveal any information. See figure 2.6² for an example for $k = 2$.

Contrary to steganography, there is no host data in visual cryptography. The secret is shared and can be extracted by combining part of the keys. The keys have visual representations (transparencies). See the papers by Naor [164], Droste [54] and Stinson [215].

REFERENCES

- [1] N. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," *IEEE Computer*, Feb. 98, p.26.
- [2] R. G. van Schynold et al, "A digital watermark", *ICIP'94*, pp.86-90.
- [3] I.J. Cox et al, "Secure spread spectrum watermarking for images, " *ICIP'96*, pp.243-246.
- [4] C. Podilchuk and W. Zeng, "Perceptual watermarking of still images," *IEEE Workshop on Multimedia Signal Processing*, June 1997, Princeton.
- [5] Chumsky
- [6] F. Hartung, B. Girod, " Watermarking of uncompressed and compressed video," *Signal Processing* 66 (1998) 283-301.
- [7] B. Mobasser, " Direct sequence watermarking of digital video using m -frames," *Proc. ICIP'98*, October 4-7, Chicago.
- [8]. D. Sarwate and M. Pursley, "Crosscorrelation properties of Pseudorandom and related sequences," *Proc. IEEE*, May 1980, pp.593-619.
- [9] Jonathan I., Su Bernd Girod," POWER-SPECTRUM CONDITION FOR ENERGY-EFFICIENT WATERMARKING," *IEEE Trans. Image Proc.*, pp. 301-305, 1999.
- [10] Jonathan K. Su, Member, IEEE, and Bernd Girod, Fellow, IEEE," POWER-SPECTRUM CONDITION FOR ENERGY-EFFICIENT WATERMARKING," *IEEE TRANSACTIONS ON MULTIMEDIA*, vol. 4, no. 4, december 2002

- [11] I. J. Cox, J. Kilian, T. Leighton, T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Proc.*, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.
- [12] M. D. Swanson, M. Kobayashi, A. H. Tewfik, "Multimedia data-embedding and watermarking techniques," *Proc. IEEE*, vol. 86, no. 6, pp. 1064-1087, Jun. 1998.
- [13] J. K. Su, F. Hartung, B. Girod, "Digital watermarking of text, image, and video documents," *Computers & Graphics*, vol. 22, no. 6, pp. 687-695, Dec. 1998.
- [14] F. Hartung, J. K. Su, B. Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks," in *Proc. SPIE Security and Watermarking of Multimedia Contents*, San Jose, CA, USA, Jan. 1999, vol. 3657,
- [15] M. Kutter, F. A. P. Petitcolas, "A fair benchmark for image watermarking systems," in *Proc. SPIE Security and Watermarking of Multimedia Contents*, San Jose, CA, USA, Jan. 1999, vol. 3657, pp. 226-239.
- [16] P. G. Flikkema, "Spread-spectrum techniques for wire-less communications," *IEEE Signal Proc. Magazine*, vol. 14, no. 3, pp. 26-36, May 1997.
- [17] C.-T. Hsu, J.-L. Wu, "Hidden signatures in images," in *Proc. IEEE Intl. Conf. Image Proc.*, Lausanne, Switzerland, Sep. 1996, vol. 3, pp. 223-226.
- [18] A. Piva, M. Barni, F. Bartolini, V. Cappellini, "DCT-based watermark recovering without resorting to the uncorrupted original image," in *Proc. IEEE Intl. Conf. Image Proc.*, Santa Barbara, CA, USA, Oct. 1997,
- [19] J. K. Su, B. Girod, "On the imperceptibility and robustness of digital fingerprints," in *Proc. IEEE Intl. Conf. Multimedia Computing and Systems*, Florence, Italy, Jun. 1999, vol. 2, pp. 530-535.

- [20] M. H. Hayes, Statistical Digital Signal Processing and Modeling, John Wiley and Sons, New York, NY, USA, 1996
- [21] G. C. Langelaar, R. L. Lagendijk, J. Biemond, pp. "Removing spatial spread spectrum watermarks by non-linear filtering," in Proc. EUSIPCO 98, 1998, vol. 4. 2281-2284.