Implementation of Watermarking Technique Using Matlab

Thesis submitted in partial fulfillment of the requirements for the award of the degree of

Master Of Engineering

In

Electronics And Telecommunication

by

CHANDRA CHUR MALLICK

Examination Roll No: M4ETC22031

Registration No.: 136202 of 2016-2017

Roll No: 002010702031

Under Esteemed Guidance

Of

Prof. Subir kumar Sarkar

DEPARTMENT OF ELECTRONICS AND TELE-COMMUNICATION ENGINEERING JADAVPUR UNIVERSITY, KOLKATA - 700032, WEST BENGAL, INDIA

June 2022

Faculty of Engineering and Technology,

Jadavpur University

CERTIFICATE

This is to certify that the work contained in this thesis entitled " **IMPLEMENMTATION OF WATERMARKING USING MATLAB** " is a bonafide work of **CHANDRA CHUR MALLICK (Exam Roll No.:__** ***M4ETC22031*****; Class Roll No.: 002010702031 ; Registration No.: 136202 of 2016-2017),** carried out in the Department of Electronics and Telecommunication Engineering, Jadavpur University, Kolkata under my supervision and that it has not been else where for a degree.

GUIDE
Prof. Subir kumar Sarkar
Jadavpur University, Kol-700032

Prof. Ananda Shankar Chowdhury
Head of the Department
Department of ETCE,
Tech. (FET),
Jadavpur University, Kol-700032

Prof. CHANDAN MAZUMDER
Dean
Faculty Council of Engg. &
Jadavpur University, Kol-700032

DECLARATION OF ORIGINALITY AND COMPLIANCE OF ACADEMIC ETHICS

I hereby declare that the thesis contains literature survey and original research work done by the undersigned candidate, as a part of her Master of Technology in ELECTRONICS AND TELECOMMUNICATION ENGINEERING.All information in this document has been obtained and presented in accordance with the academic rules and ethical conduct.

I also declare that as required by the code of conduct, I have fully cited and referenced all material and results that are not original to this work.

Name

Examination Roll No. :

University Registration No.:

Thesis Title: "”

(Signature with date)

Faculty of Engineering and Technology,Jadavpur University

CERTIFICATE OF APPROVAL*

This is to certify that the Master Thesis entitled " ***Implementation of Watermarking using Matlab****" is hereby approved as a creditable study of an engineering subject carried out and presented in a manner satisfactory to warrant its acceptance as pre-requisite to the degree for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or accept every statement made, opinion expressed, or conclusion drawn therein but approve the thesis only for the purpose for which it has been submitted.*

Committee on Final

Examinationfor

Evaluation of the Thesis

Examiners

*Only in case the thesis is approved

IMPLEMENTATION OF WATERMARKING USING USING MATLAB

MASTERS OF ELECTRONICS AND TELE-COMMUNICATION ENGINEERING

BY

CHANDRA CHUR MALLICK

EXAM ROLL NO : M4ETC22031

REGISTRATION NUMBER : 136202 OF 2016-2017

UNDER THE ESTEEMED GUIDANCE OF

PROF. SUBIR KUMAR SARKAR

***DEPARTMENT OF ELECTRONICS AND TELE-
COMMUNICATION ENGINEERING
JADAVPUR UNIVERSITY , KOLKATA -700032
WEST BENGAL , INDIA***

ABSTRACT

Everyone uses the internet for their personal or professional use. Due to this it is important to protect user data from unauthorized access. When we talk about copyright protection means an unauthorized person claims that copied data was created by him. What do we do at that time? How can we prove that we are the right owner of data? To overcome this problem Digital watermarking mechanism is used to protect data from illegal copies or illegal distribution. It is an art of hiding information into digital data in a way , unauthorized people can’t access or copy that data for misuse. Data which is inserted into digital media is called watermark. It is information (any label, citations, author name, id) about data. The proposed paper is an analysis of new enhancements in digital image watermarking techniques in both spatial domain and transform domain.

ACKNOWLEDGEMENT

I would like to profusely thank my guidance Prof. Subir Kumar Sarkar for his patience , enthusiasm, motivation and guidance . I attribute the level of my Masters degree to his encouragement and without his guidance with immense knowledge and experience in research, my thesis would not have been completed or written .

CONTENT

TABLE OF FIGURES

IMPLEMENTATION OF WATERMARKING TECHNIQUE USING MATLAB

INTRODUCTION AND ORGANIZATION OF THE THESIS

1. THE HISTORICAL PERSPECTIVE OF WATERMARKING

From the historical point of view the art of paper making was introduced during the Chinese empire 1000 years ago. But the first evidence of paper watermarks appeared in ITALY around 1282. Although the purpose of the earliest watermarks is uncertain.However it was not until 18 th century when watermark gained its popularity, during this era watermark was used as trademarks,to record the date when the paper was manufactured and to indicate the size of the sheet.The term watermark may have originated from the german term ‘wassermarke’.

The invention of the dandy roll in 1826 by John Marshall revolutionized the watermark process and made it easier for producers to watermark their paper.

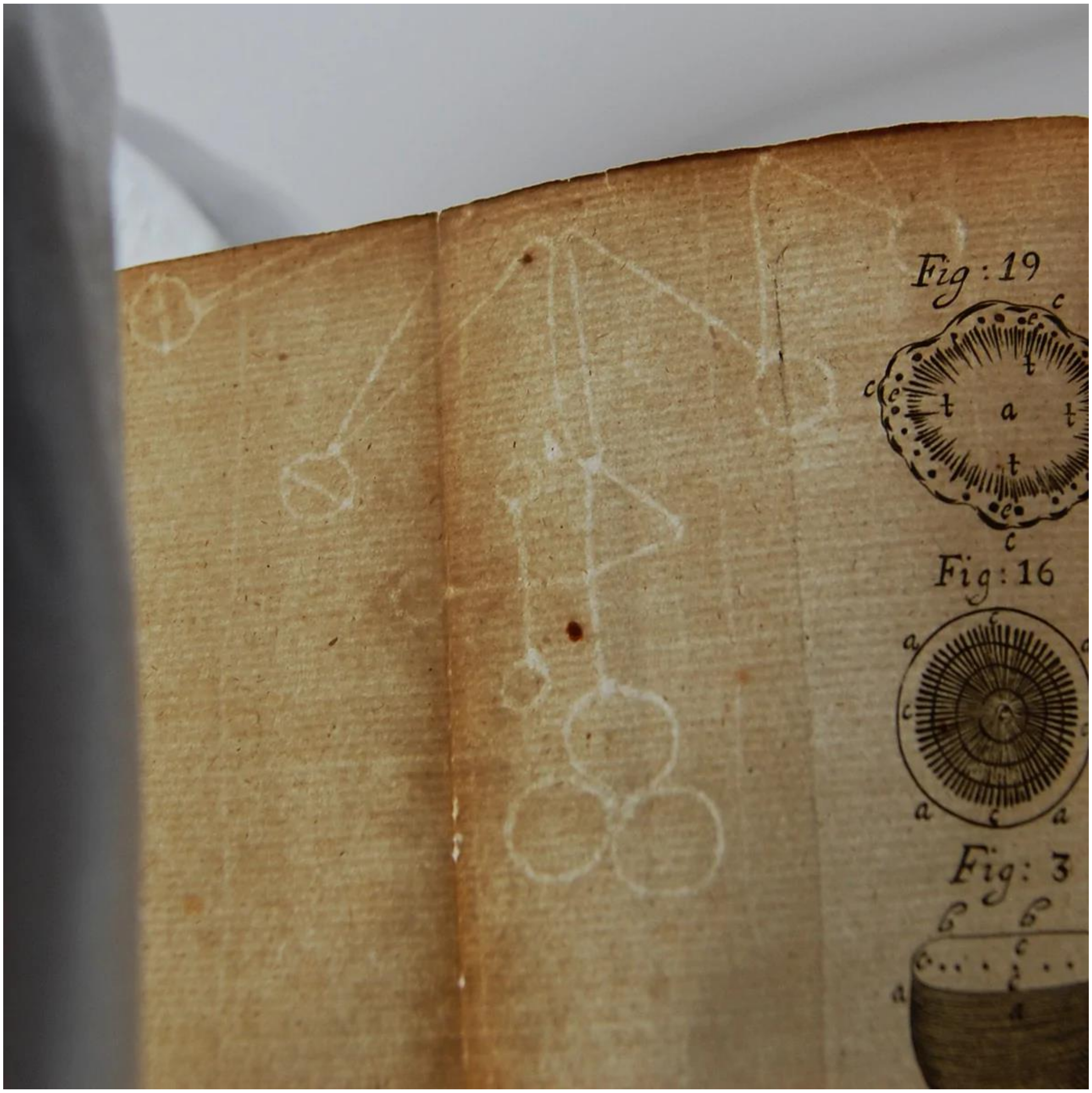


Fig 1 : first work of scientific botany

WATERMARKS & FOOLSCAPS: EXPLORING THE HISTORY OF PAPER PRODUCTION

A wire mesh mold was lowered into this mixture and lifted out several times. As the water drained through the mesh it deposited thin layers of fibers on the mold. You can see evidence of the wire mesh in the image above: the vertical lines (the ones that look like the watermark, not the folds in the paper) are called chain lines, and the more frequent horizontal lines are called laid lines. They appear when light is shining from behind because the paper is thinner in the places where a wire was. The watermark is simply created by attaching a decorative design made of thicker wire to this grid. Below is a 17th-century depiction of papermakers at work, as reproduced in Dard Hunter's *Papermaking: The History and Technique of an Ancient Craft*.

It has been around for centuries and is commonly used in money and stamps to assist in identifying counterfeiting. The idea behind watermarking is to create a translucent image on the paper to provide authenticity. Since mailing letters was far more expensive centuries back, it was common for people to use counterfeit stamps on their mail. For example, a translucent elephant watermark was used on stamps in India to deter counterfeiting.

Various watermarks are also added to money at the time of manufacture. For example, many denominations of paper money in the United States contain a watermark of the individual printed on the money. For example, on the $100 dollar bill, you will find a watermark of Benjamin Franklin if you illuminate the bill from behind

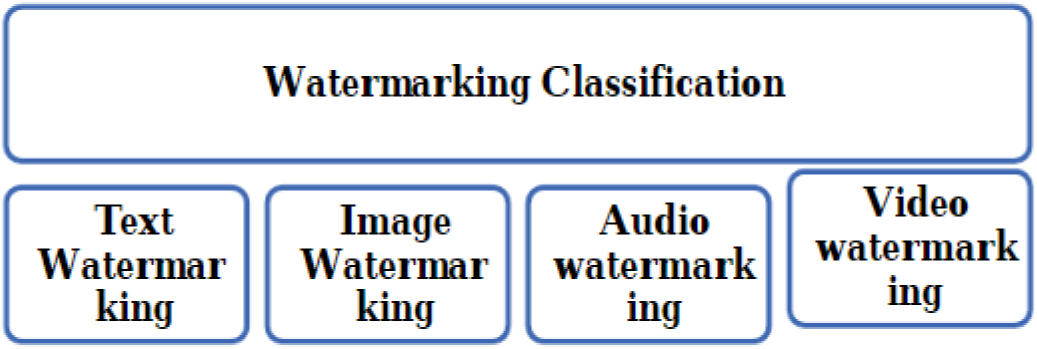
<u>Fig 2 :   In the $100 dollar bill the watermark of Benjamin Franklin is there</u>.

Digital watermarking is used to maintain ownership and authenticity of digital media such as music and videos.

It is important to note that although watermarking has many similarities to steganography in terms of embedding data, but the intent of watermarking is not to make it difficult to detect that embedded data, but rather make it difficult to remove the embedded data so as to prevent the unauthorized reuse of the file.

Fusion of Watermarking and Steganography for Protecting Image Ownership

Watermarking is a technique of inserting the information to the different digital media for example image, video
or audio that provides the data authentication and copyright protection . By using digitalwatermarking technique, the owner of digital media can protect the copyright of the file. Figure 1 shows the different
watermarking classification which are text watermarking, image watermarking, audio watermarking and video
watermarking.
Text watermarking is used to operate as a watermark text in the image. It can have applied in the layout and
background of appearance of the image. Image watermarking is used to hide any secure image.
Audio watermarking is a single which is inserted as watermarking into audio singles. Video watermarking is used to security
the videos which are divided into different video shots and after that, each shot selected one video frame. This video
A frame in image processing is called an identical frame.



<u>Fig 3 : classification of watermarking</u>

TEXT WATERMARKING

The copyright of text documents are infringed by illegal copy and distribution. Watermark is one of the approaches for text document copyright protection. Watermark is used commonly in monetary currencies to make counterfeiting more difficult. A watermark can be a variety of objects such as an image, or some copyright information. A watermark is some data that can be extracted later as a proof of the copyright of the document in the situation of a digital document. Text watermarking is a process to embed a watermark into a text document. The watermarks can be divided into two types: visible and invisible, and is associated with human vision. The watermark discussed in this paper is invisible. It is some data embedded into a text document that can pass easily from one copy to another copy. Therefore, the watermark works like a token that allows the copyright owner to detect illegal copies and prosecute the copyright violator who may be the seller or the owner of the illegal copy. If a text document is a long document, and then the copyright protection system assigns a secret key to the copyright owner. The system keeps the record of the secret key, and even a copy of the document. A watermark embeds into a text document by the secret key; therefore the secret key can be used to extract the watermark from the text document. The copyright owner may have one or more secret keys, but he had to keep recording which key for which text document.

IMAGE WATERMARKING

Image watermarking is embedded text or logos over a digital image. This watermark graphic or text indicates ownership or copyright of the image. It makes it difficult for someone to use the image without permission or claim ownership of the original. It’s typically in the corner of the image but can be anywhere across the photo.

VIDEO WATERMARKING

Watermarking is the process of covertly embedding some kind of “signal” into a piece of content to help identify the ownership, copyright, and/or authenticity of a given piece of content. For the purposes of this post – we’ll focus on digital images and video content, although watermarks are also used for print and audio content as well. Video watermarking can be broken down into two categories – perceptible and imperceptible. Perceptible watermarks usually involve superimposing a logo or text over a piece of content.

In some cases the perceptible video watermarks can simply include a logo of the video player, brand, or broadcast service, similar to the example from Bitmovin’s Player:

On the other hand, just applying a logo or a watermark overlay often isn’t enough to actually deter piracy. For that, we'll need to use the more powerful alternative, imperceptible video watermarking. Metadata such as User ID, device ID, IP address, and time stamps, can be embedded within imperceptible video watermarks and used as forensic evidence to track down the source of piracy and leaks. As you can see in the image below, the imperceptible video watermark is applied using a back-end identifier and is completely transparent to the end client.

Taking this one step further, there are two types of imperceptible watermarking solutions, client-composited watermarking and server-side watermarking. Client-composited watermarking is applied on a given consumer's device such as set-top boxes, OTT clients or applications, mobile or tablet devices, and smart TVs, while the server-side forensic watermarking solution is integrated with the video processing platform.

Client-composited forensic watermarking solution

Client-composited watermarking is one of the most commonly applied methods for live sports due to the faster watermark extraction cycle. In most cases, a content provider can apply client-side watermarks during playback via code or third-party libraries integrated with their player.

There are a couple of caveats to client-side watermarking:

1. Custom integrations are necessary for each unique device or player
2. It often requires code obfuscation technology on top of the client-composited watermarking solution to prevent reverse engineering and blocking the watermark insertion process.

Server-side forensic watermarking :

Server-side forensic watermarking is applied at the encoding and packaging stage of the content delivery process, often creating two copies of every file, with distinct

“A” and “B” watermarks. For ABR streaming, the A/B watermarking process is applied as follows:

1. Video content is broken down into chunks (segments)
2. During the encoding process, segments are duplicated and embedded with distinct Watermark A and Watermark B variants
3. Both A and B segment variants are output and stored for delivery by a CDN
4. When a player requests segments, the CDN sends a unique combination of A and B segments to each player, (ex: Customer #1 gets ABABA, Customer #2 gets ABBAA, Customer #3 gets BBBAA)

5. The Watermarking Provider’s Detection Service uses the pattern of A/B segments in a pirate stream to identify the session and subscriber responsible for the leak and take appropriate action.

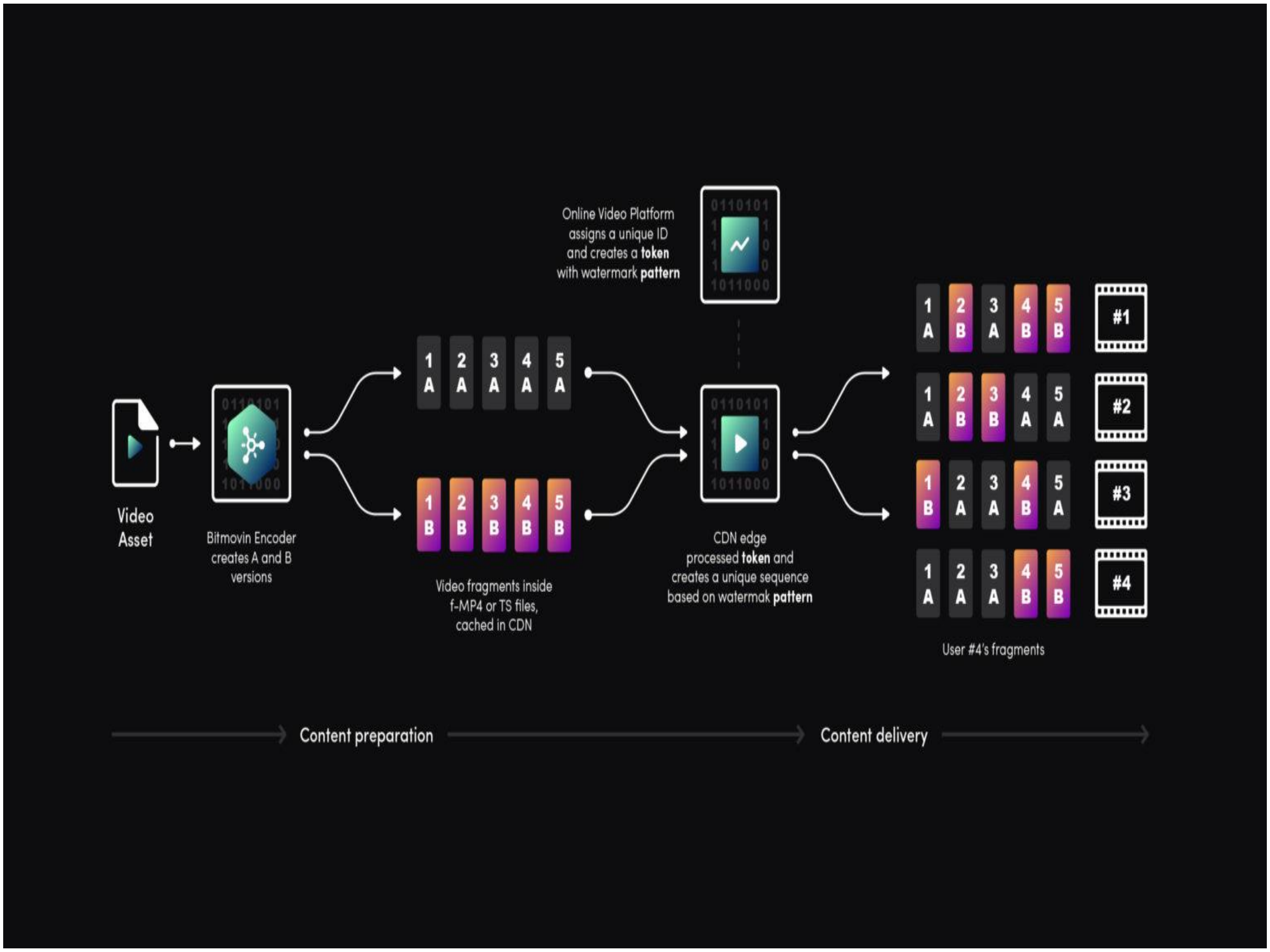


FIG 4 : A/B Video Forensic Watermarking in Bitmovin's Encoding

THE LINK WITH CRYPTOGRAPHY WITH AND WATERMARKING

Cryptography is defined as the art and science of secret writing.The word itself comes from the Greek word kruptos and graphen mean secret and writing,respectively.The focus in crypto is to protect the content of the message and to keep it secure from unintended audiences

It is quite visible that the concept of cryptography and watermarking are closely derived and both can be communicated in hidden form.In cryptography , the message is usually scramble and unreadable.However, when the communication happens.Although the information is hidden in the cipher, an interception of the message can be damaging.The major difference between cryptography and watermarking is cryptography has no way of preventing and tracking the misuse which defies the very purpose of watermarking.Tracking and prevention of the illegal distribution of data is one of the main purpose of digital watermarking.

There are surely many advantages of cryptography but from the point of view of copyright protection,broadcast monitoring etc. Watermarking is a form of digital watermarking on digital media in the eve of the 21st century is the best fitted solution.

DIGITAL IMAGE WATERMARKING

Digital Watermarking is the process of inserting meaningful information within a host in a way that may or may not ‘perceptible’.In other words watermarking is defined as adding a payload signal to host signal.The payload can be detected or extracted late to make an assertion about the project i.e. the original data that may be an image or audio video.

Frequently used term in digital watermarking .

HOST : The image ,audio,video or any other media in which the information is to be inserted.

Watermark : it is the information which may be unique or may not be unique which is to be inserted within the host . It might be an image , a random sequence,multiple- bit information etc.The watermark might contain some information about the authenticity of the host or content of the host etc. Usually, the tenacity of the watermark to remain undistorted despite of intentional and unintentional changes brought about in the host or the inclination of the watermark to change as a result of any small or large distortion introduced in the host are the major principles that govern the technique of digital watermarking.

Stego: The image,the audio,video, multimeter or any other media formed as a result of the watermark being within the host is known as stego.

BROAD CLASSIFICATION OF WATERMARKING TECHNIQUES

Visible watermarks: A visible alteration of the digital image by appending a “stamp” on the image is called a visible watermark. This technique directly maps to that of the pre-digital era where a watermark was imprinted on the document of choice to impose authenticity.

Invisible watermarks: By contrast, an invisible watermark, as the name suggests , is invisible for the most part and is used with a different motive. While the obviousness of visible watermarking makes distinguishing legitimate and illegitimate versions easy, its conspicuousness makes it less suitable for all applications. Invisible watermarking revolves around such suitable factors that include recognizing authentic recipients, identifying the true source and nonrepudiation.

Fragile watermarks: These are complementary to robust watermarks and are, as a rule, more change-sensitive than robust watermarks. They lose their mettle when they are subject even to the smallest changes. Their use lies in being able to pin-point the exact region that has been changed in the original watermarked image. The methods of fragile watermarking range from checksums and pseudo-random sequences in the LSB locate to hash functions to sniff any changes to the watermark.

Semi-fragile watermarks: These watermarks are a middle ground between fragile watermarks and fragile watermarks. They engulf the best of both worlds and are more resilient than fragile ones in terms of their robustness. They also are better than robust watermarks in terms of locating the regions that have been modified by an unintended recipient.

Robust watermarks: By hypothesis robust digital watermark repeals all types of attacking techniques on the watermark . Watermarks can be used to hold knowledge of ownership. Such watermarks need to remain steadfast to the original image to do what they advertise. The intactness of the watermark is a measure of its robustness. These watermarks must be able to withstand normal manipulations to the image such as reduction of image size, lossy compression of image, changing the contrast of the images, etc.

Digital watermarks are also spatial and spectral watermarks

Spatial watermarks: Watermarks that are applied to the "spatial domain of the image" are said to be spatial watermarks

Spectral watermarks: These are watermarks that are applied to the "transform coefficients of the image"

The Watermarking Process

The watermarking process comprises of the following stages

1. Embedding stage

2. Extraction phase

3. Distribution stage

4. Decision stage

Embedding stage: In this stage, the image to be watermarked is preprocessed to prime it for embedding. This involves converting the image to the desired transform. This includes the discrete cosine transform (DCT), the discrete Fourier transform (DFT) and the wavelet domains. The watermark to be embedded may be a binary image, a bit stream or a pseudo-random number that adheres to, say, a Gaussian distribution. The watermark is then appended to the desired coefficients (low frequency or intermediate frequency) of the transform, as recommended by Human Visual System (HVS) research. The watermarked image is the output of this process and is obtained by performing an inverse transform on the altered transform coefficients .

Distribution stage: The watermarked image obtained above is then distributed through digital channels (on an Internet site). In the process, this may have undergone one of several mappings, such as compression, image manipulations that downsize the image, enhancements such as rotation, to name a few. Peter Meerwald refers to the above as “coincidental attack”. Any of the above may put the watermarking scheme to test, as we will see in the ensuing section. In addition, malicious attacks also are possible in this stage to battle with the watermark. These are referred to in Meerwald's work as "hostile attacks".

Extraction stage: In this stage, an attempt is made to regain the watermark or signature from the distributed watermarked image. This stage may need a private key or a shared public key, in combination with the original image, or just the watermarked image.

ATTACKS ON DIGITAL WATERMARKING

There are different kinds of attacks which affect a watermarked image when in use on different platforms such as the internet. It is desirable a watermarked algorithm must resist a subset of practical level such kinds of attacks . Although it is not expected that a digital watermarking algorithm will be resistant to a huge amount of such attacks since then the quality of the original image will be so distorted that it will be of no use whatsoever.

Copy attack: This attack is viable through obtaining a legitimate watermark from a watermarked content and copies or embeds it into another carrier signal (an unwatermarked work). As the definition implies, this attack requires performing a removal attack or carrying out some kind of estimation (using prior knowledge of signals' statistics, having the same host signal carrying different watermarks and etc.) to extract the Watermark.

Oracle attack: An attacker is able to launch an oracle attack without knowledge about the algorithm only by using a watermarked digital content, if he/she has a detector at his/her disposal. In this attack, the attacker has the opportunity to apply few modifications to the work and figure out whether it is inside the detection region or not. Repeating this process (i.e. altering the work and testing) provides the adversary with valuable knowledge regarding the operation of the detection algorithm. Two well-known attacks namely, sensitivity analysis attack and Gradient descent attacks are considered in this category.

Sensitivity analysis attack utilizes a binary decision (i.e. yes or no) about the existence of the watermark, while gradient descent attack exploits the values of the detection statistic. Spread spectrum watermarking schemes are vulnerable to sensitivity analysis attacks.

Ambiguity attack: This attack sometimes called IBM attack or Craver attack and it aims to puzzle the detector by generating fake watermarks from a watermarked work. Thus, it leads to ambiguity in the ownership of the media content. The vulnerability that enables this kind of attack is related to the concept of being invertible in the watermarking system. In fact, being non-invertible (i.e. the inverse of embedding is computationally implausible) regarded as one of the preferred requirements that a watermarking scheme should possess. A possible countermeasure is to make watermarks signal-dependent by using cryptographic hash functions.

APPLICATION OF DIGITAL WATERMARKING

Digital Watermarking has been a major breakthrough for the protection of copyright material in digital form .Due to the application of it in all kinds of media such as audio,video,image,document,and for quite large application domain such as broadcast monitoring copy control,authentication it has emerged as an important field of research.

Owner Identification: In many countries of the world creation of story ,painting , song or any kind of original work automatically holds copyright to the instant it is stored in any form of physical media.It is sometimes the standard 'c' notice helps us along with its owner identification help us to recognize it is a copyright material . The exact form of copyright notice varies in different forms. As because watermark is inseparable and imperceptible from its original work they are more likely to superior to the text for owner identification .Digimarc is a well known popular watermark detector bundled with the Adobe Photoshop , it contacts with the central database over the internet to find the owner information , it is a good example of owner identification application of digital watermarking .

Broadcast Monitoring :

The application of digital watermarking in the context is to monitor the actual broadcast of advertisement . There are many organizations or individuals interested in monitoring the broadcast due to the scandal broke in 1997 by a Japanese television channel. Advertisers want to ensure they receive all of the airtime they purchased form the broadcaster this made necessary the airtime monitoring through the content verification or the broadcast monitoring . The manual broadcast monitoring is very simple but error prone. Here the observer hears what is broadcasting and records what is broadcasting and records what they see and what they hear .In general there are two types of broadcasting monitoring active and passive . Passive monitoring tries to directly recognize the content being broadcasted .However there are many potential problem in passive monitoring one such is comparing the received signal against the database is not trivial which is done in passive monitoring while active monitoring relies on the information broadcasted along with the actual content . Technically active monitoring is easier to implement .

A unique watermark can be embedded in the video or the audio segment to verify the broadcast . Automated monitoring station is installed to verify when and where the watermark clip appears.

Proof of Ownership :

The object here is not just to identify the copyright ownership but to actually prove it . In scenarios such as an un-authenticated user may steal an image from the original owner and after removing the watermark of the original owner he replaces it with his own watermark and claims to be the original creator . In case of such ambiguity the only way to restrict the forgery is to restrict the availability of the detector .

Transaction Tracking :

Here the watermark is implemented to record the no of transactions or the no of copy made from the original one .

For example the watermark might record the recipient for each legal distribution of the work . If the owner embeds different watermarks in the copy then he may track which user is liable to forgery , misuse or an unauthenticated use.Transaction tracking is often called fingerprinting in as each copy of the stego can be uniquely identified by the owner which is same as unique property of fingerprint .This application of digital watermarking is potentially valuable both as deterrent to illegal use and as a technological aid to investigation.

Content Authentication :

Sometimes it is possible to edit an original image to an extent that even after removing some valuable information from the image , the edited seems in anked eyes as though that information does not exist in the original one . Had it been serious evidence then this could lead to misinterpretation of the original fact . In order to prevent such kind of casualty content authentication should be introduced which is implemented by the application of watermarking by using an authentication mark . The fragile watermarking is the particular solution generally used to solve the problem, this kind of watermarking identifies even the slightest measure of change occurring in the stego. Although signature is an alternative solution to the problem but it suffers from the drawback such as file conversion , digital signature is stored as metadata and during conversion from one format to another the metadata gets lost. A more advanced form of content authentication purpose Epson implemented the watermarking system in its camera.

Copy control :

To prevent illegal control of copyright material copy control mechanism is implemented >encryption is a strongest form of defense to control copy mechanism.Due to some disadvantage of method such as requirement of key which can be obtained by searching or by registration one time as an authentication user etc. The concept here is to implement a no copy watermark on the material concerned which will indicate the program which is running it as an unauthenticated user.

Device Control :

The copy control falls in the larger domain of device control . There are several instances where devices react to the watermark when they detect the content . It is somewhat different with respect to copy control as it adds some value to the content concerned rather than restricting its use.

PHASE CONGRUENCY IN WATERMARKING

Phase Congruency (Kovesi, 1996) is an alternative measure of local feature detection in image, it is assumed to be one of the strongest methods as it outputs a dimensionless quantity which is particularly independent of changes of illumination and contrast.

A Phase Congruency based digital color image watermarking algorithm is proposed which provides a higher degree of robustness against attacks and excellent imperceptibility. Here, Phase Congruency has been used to detect the local feature regions of the host image and then the watermark has been infused into it using a new technique called 'Adaptive α-β Blending'. An accurate Human Visual System modeling has been incorporated via Lifting Wavelet Transform to take the full advantage of perceptual watermarking. The coefficients of the α-β blending are selected adaptively based on the Phase Congruency feature map of the host image. Furthermore, the watermark is secured with a cryptographic algorithm called Arnold's Cat Map to prohibit further eavesdropping. From rigorous testing, results indicate that our approach is robust against various geometric, non-geometric and combined attacks while maintaining a sublime imperceptibility.

Local Energy and Phase Congruency

The local energy model of feature detection postulates that features are perceived at points of maximum phase congruency in an image. For example, when one looks at the Fourier series that makes up a square wave, all the Fourier components are sine waves that are exactly in phase at the point of the step at an angle of 0 or 180 deg. depending on whether the step is upward or downward. At all other points in the square wave, phase congruency is low. Similarly, one finds that phase congruency is a maximum at the peaks of a triangular wave (at an angle of 90 or 270 deg.). Congruence of phase at any angle produces a clearly perceived feature.

$s(x) = \sum_0^n \quad (1/(2n+1))$ (sin[2n+1]x + ϕ)

Where ϕ the offset at which congruence of phase occurs varied from 0 to □/2.

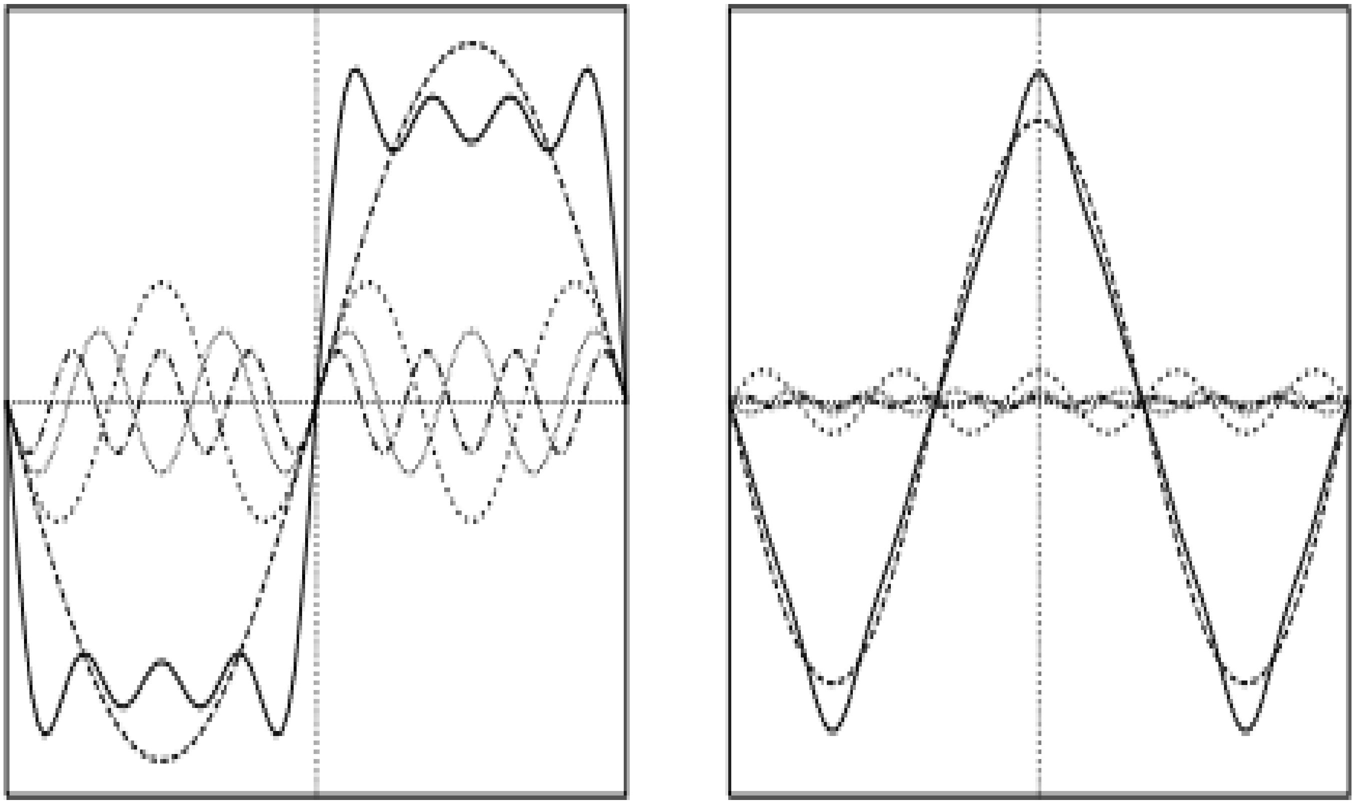


Fig 5 : Construction of square and triangular waveforms from their Fourier series. In both diagrams, the first few terms of the respective Fourier series are plotted with broken lines; the sum of these terms is the solid line. Notice how the Fourier components are all in phase at the point of the step in the square wave, and at the peaks and troughs of the triangular wave.

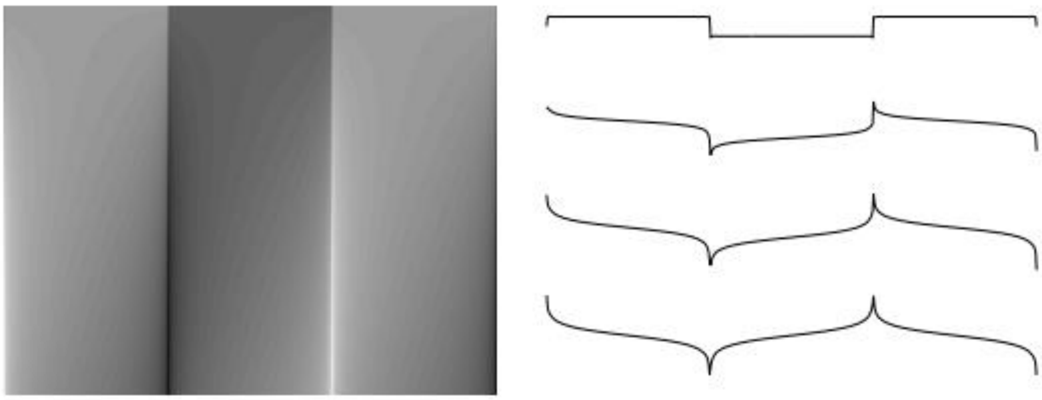


Fig 6 : Interpolation of a step feature to a line feature by continuously varying the angle of congruence of phase from 0 at the top to π/2 at the bottom. Profiles of this grating corresponding to congruence of phase at 0, π/6, π/3, and π/2 are shown on the right.

The local energy function is directly proportional to the phase congruence function, so peaks in local energy will correspond to peaks in phase congruency.
The relationship between phase congruency, energy, and the sum of
The Fourier amplitudes can be seen geometrically in Figure 7. The local

Fourier components are plotted as complex vectors adding head to tail.

The sum of these components projected onto the real axis represent

F (x), the original signal with DC component removed; the projection

onto the imaginary axis represents H (x), the Hilbert transform. The

magnitude of the vector from the origin to the end point is the total energy, E(x). One can see that E(x) is equal to

n Ancos(φn(x) − φ(x)).

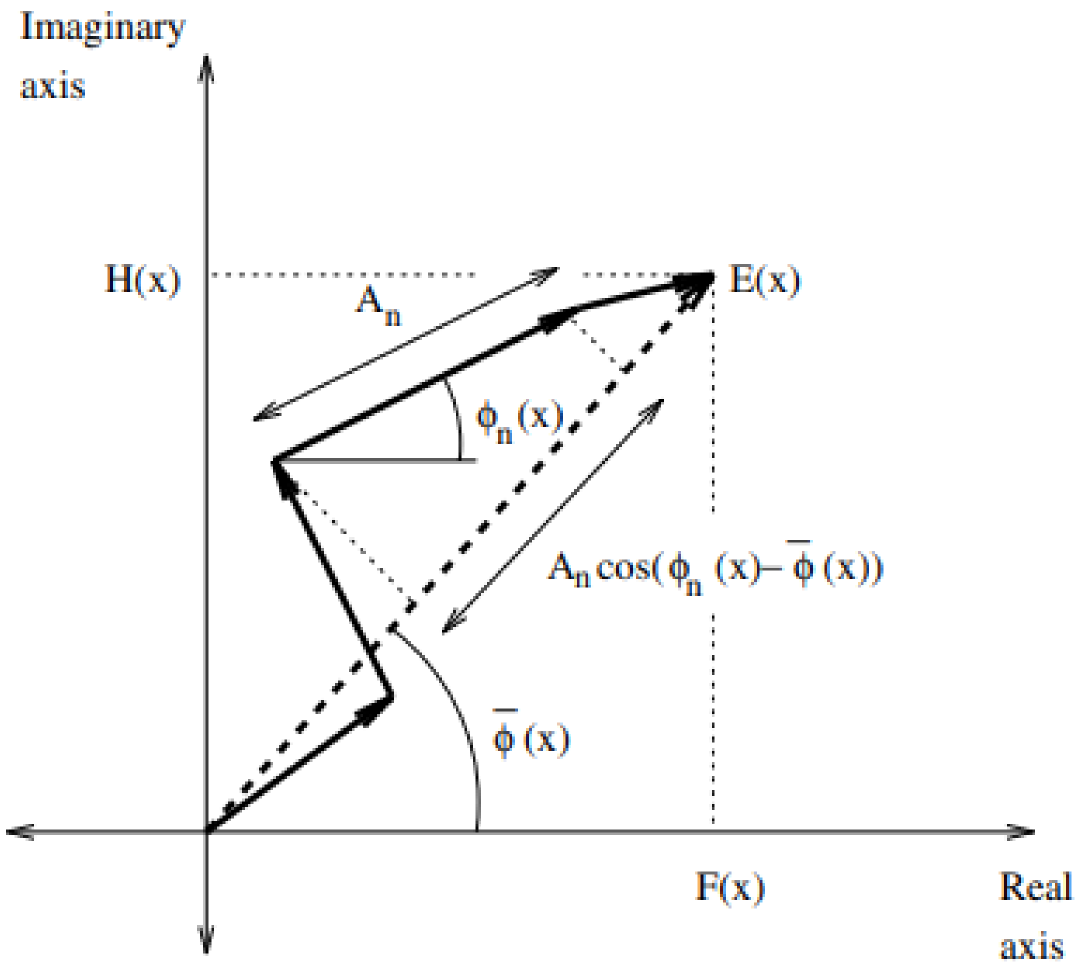


Figure 7. Polar diagram showing the Fourier components at a location in the signal plotted head to tail. This arrangement illustrates the construction of energy, the sum of the Fourier amplitudes, and phase congruency from the Fourier components of a signal.

Phase congruency is the ratio of E(x) to the overall path length taken by the local Fourier components in reaching the end point. Thus, one can clearly see that the degree of phase congruency is independent of the overall magnitude of the signal. This provides invariance to variations in image illumination or contrast.

SINGULAR VALUE DECOMPOSITION

The Singular Value Decomposition (SVD) is a practical numerical tool with applications in a number of signal processing fields including image compression. In an SVD-based watermarking scheme, the singular values of the cover image are modified to embed the watermark data.

INTRODUCTION

o the highly networked societies that we live in today communication has always been an integral part of our existence. Methods of communication today include radio communication, telephonic communication, network communication and mobile communication. All these methods and means of communication have played an important role in our lives, but in the past few years, network communication, especially over the internet has emerged as one of the most powerful forms of communication with an overwhelming impact in our lives. With the advance in technology, illegal operations in digital media have become easy. Therefore, copyright protection has become an important issue. One of the solutions for this problem is the embedding of digital watermarks into the data. Watermarking is the process of embedding a watermark into an object. This object may be audio, video or image. To get more effective output, the water should be perceptually invisible, difficult to remove without seriously affecting the image quality and should robustly resist image distortions caused by attacks such as common image processing operations and lossy image compression.Several watermarking techniques have been proposed. These techniques can be classified into two: spatial domain techniques and frequency domain techniques. In spatial domain technique which embed the data directly by modifying the pixel values of the original image. In frequency domain technique which embeds the data by modulating the coefficients of a properly chosen transform, Watermarking techniques covers a wide area. Many other techniques were also proposed. Example cryptography, security through quantization ,discrete cosine transform.A new method of watermark detecting is proposed in . In this a Gaussian distribution is assumed in DCT and DWT domains. Most commonly used methods of watermarking are Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT),and Discrete Fourier Transform (DFT). These transform domain techniques always give more robust output SVD and DCT based watermarking schemes as explained in SVD is a powerful numerical analysis tool for matrices which give minimum least square truncation error. This is because the total potential degrees of freedom of three matrices are equal to the input host image, also explaining the SVD based image watermarking scheme, which gives secure and robust owner identification. The main properties of SVD image processing are i. The singular values of an image have good stability ii. Singular values represent intrinsic algebraic image properties. In this paper, we propose an improved SVD based image watermarking scheme. Unlike other transforms which use fixed orthogonal bases, SVD uses non fixed orthogonal bases. The result of SVD gives good accuracy, good robustness and good imperceptibility in resolving rightful ownership of watermarked images.

The Watermark Embedding Procedure

In the proposed watermarking scheme the input image is gray scale.

Step 1: Partition the image into blocks of n×n pixels

Step 2: Apply SVD transformation to each partitioned block

Step 3: Calculate the number of non-zero co-efficient in the D component of each block. This is calculated to determine the complexity of the block.

Step 4: Select greater complexity blocks using PRNG [pseudo random number generator] and also using the feature of D component.

Step 5: For each selected greater complexity block, in the first column of U, magnitude difference between the neighboring coefficients is calculated.

Step 6: First, if the magnitude difference matches the embedding watermark (e.g. positive relationship matching a bit value of 1 or negative relationship matching a bit value of 0), the coefficients are retained. Second, if the magnitude difference does not match the embedding watermark, the coefficient must be modified.

Step7: To retain the image quality and provide a stronger robustness of a watermarking scheme, the difference value is first checked to be above a certain threshold.

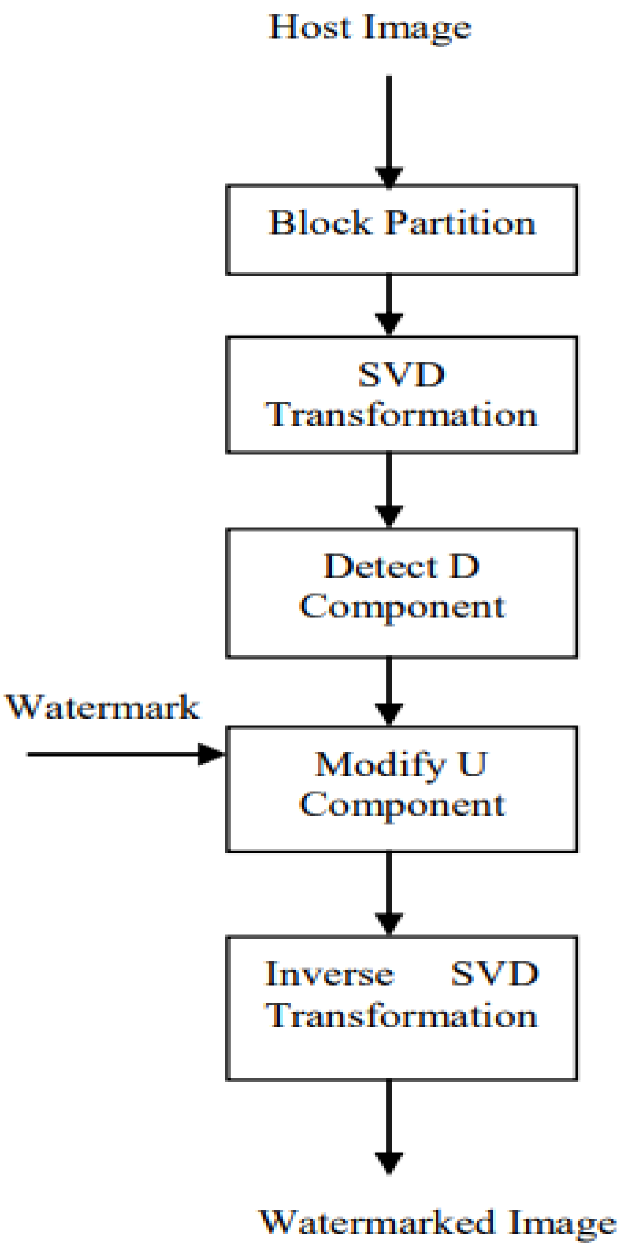


Fig 8: water embedding procedure

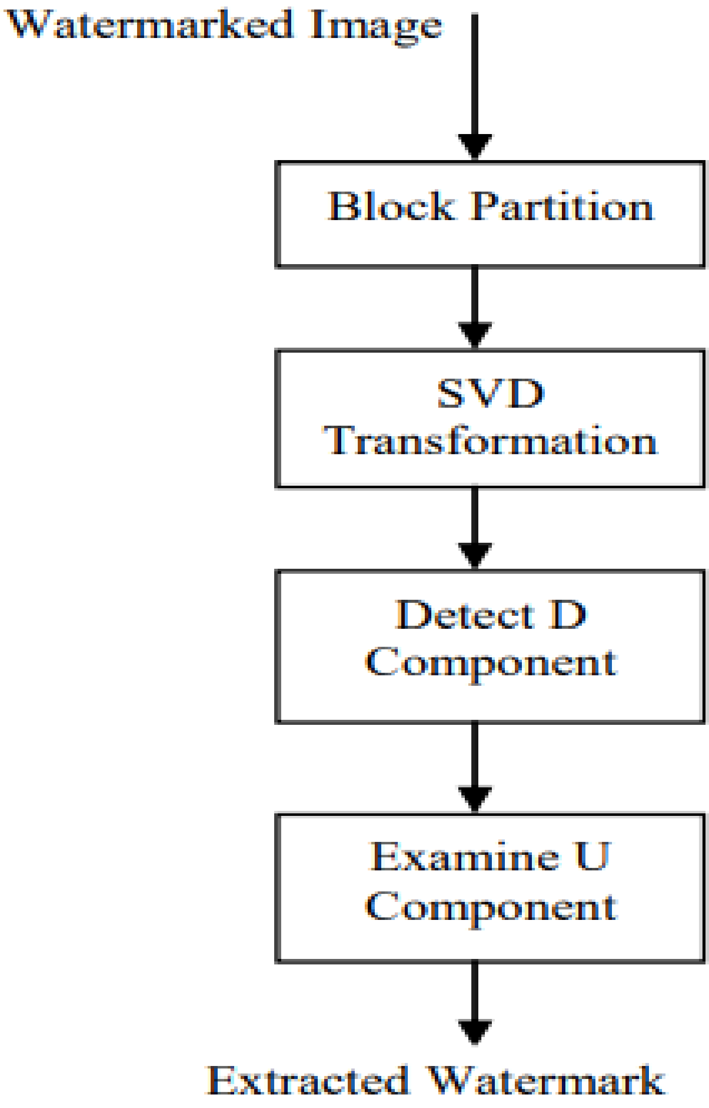


Fig 9: water extraction procedure

THE WATER EXTRACTING PROCEDURE

The watermark extraction procedure is similar to the watermark embedding procedure.

Step1: Block partitioned the watermarked image

Step2: Apply SVD transformation to these block partitioned pixels

Step3: Calculate the number of non-zero co-efficient in the D component of each block. This is calculated to determine the complexity of the block.

Step4: Using the feature of D component and PRNG, the relationship of U component is calculated

Step5: If a positive relationship is detected, the extracted watermark is assigned a bit value of 1. Otherwise, the extracted watermark is given a bit value of 0.

SVD can be used for face recognition techniques . SVD acts on the basis of an approach called “face space” , spanned by a group of “base space” .”face space” is a subspace of vectors and the vectors are the set of known faces. The approach is similar to Principle Component analysis recognition is performed by projecting a new image onto the facespace then comparison of coordinates with known faces is done to classify the face . However SVD turned out to be better performance than PCA.

- The singular values obtained from an image hold the property of luminance and the geometric information of the image .

- Variation of intensity has less effect on singular values of image .

- Perhaps one of the most important aspects trending on SVD applications is the watermark embedding . Thus an image can be more informative without a significant loss of image visual quality . SVD is inherently JPEG compression resistant , it is also consistent with several watermarking attacks like scaling , translation, transpose etc.

RESULTS AND DISCUSSION

In order to demonstrate watermarking   using matlab , I used two images for trial during my thesis

Discussion – 1.0 :

In Figure 10 , the image where the watermark is to be inserted so that to assist in identifying counterfeit .Watermarking helps us to protect our images **.** We can add a visible watermark to your digital images and photos to protect intellectual property.

When organizations leave their digital assets unprotected, they can face serious implications, including asset misuse, brand depreciation, and legal fines. Additionally, with the number of resources being spent to create original content, plus the repercussions of misuse , to safe these important credentials

And datas from third parties we must protect our data from getting surfaced across the board.

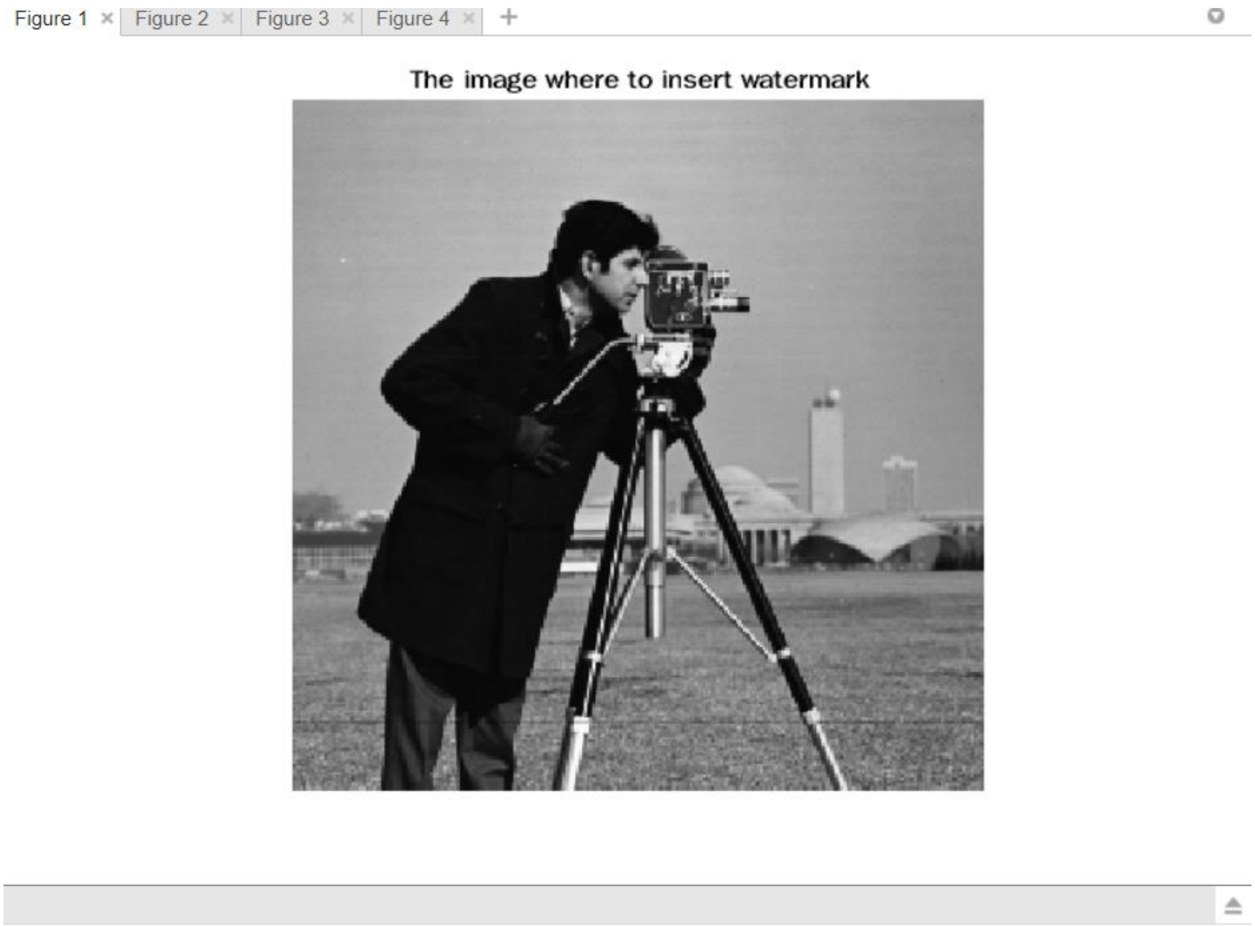


Fig 10 : Original image where the watermark is to be inserted

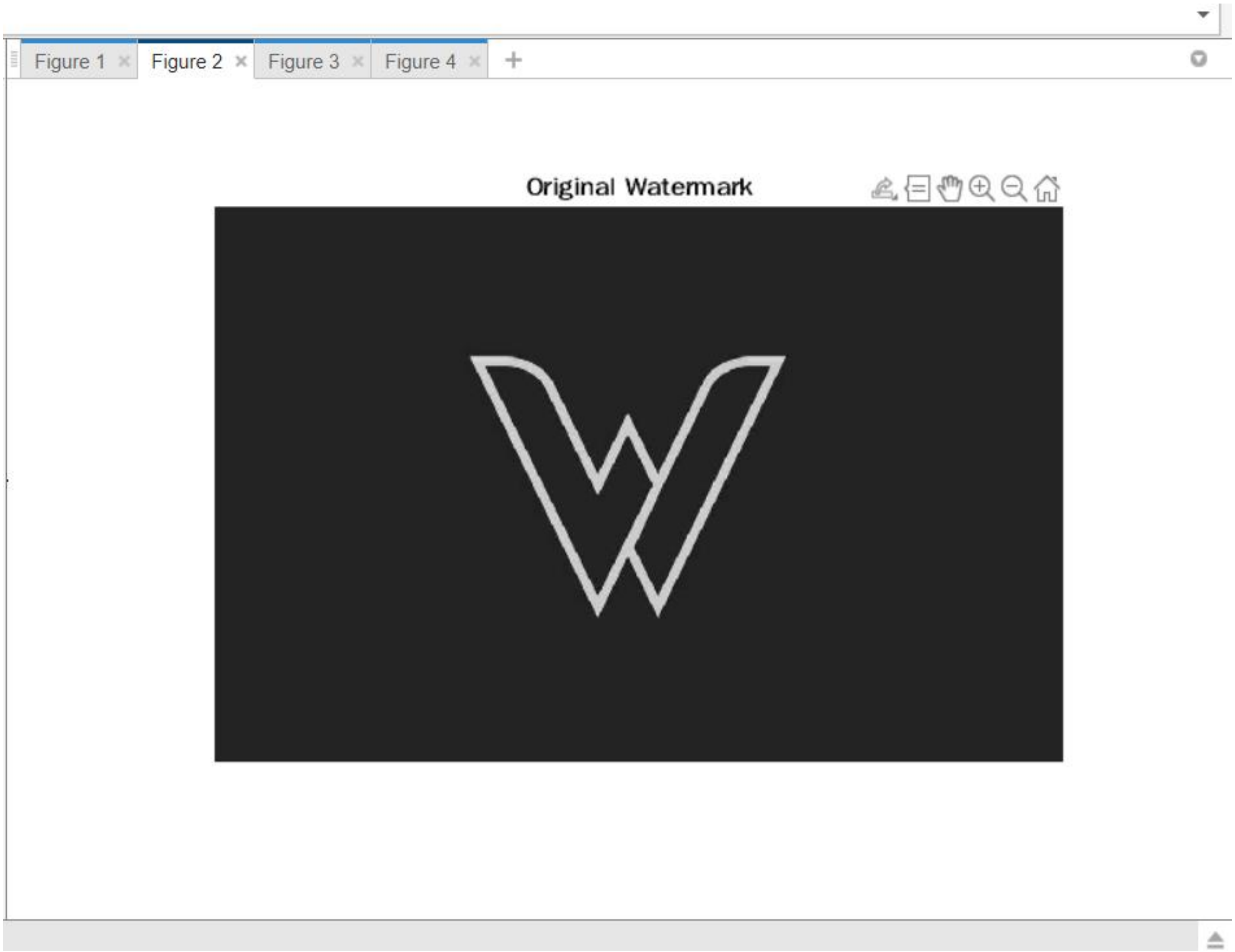


Fig 11 : original watermark

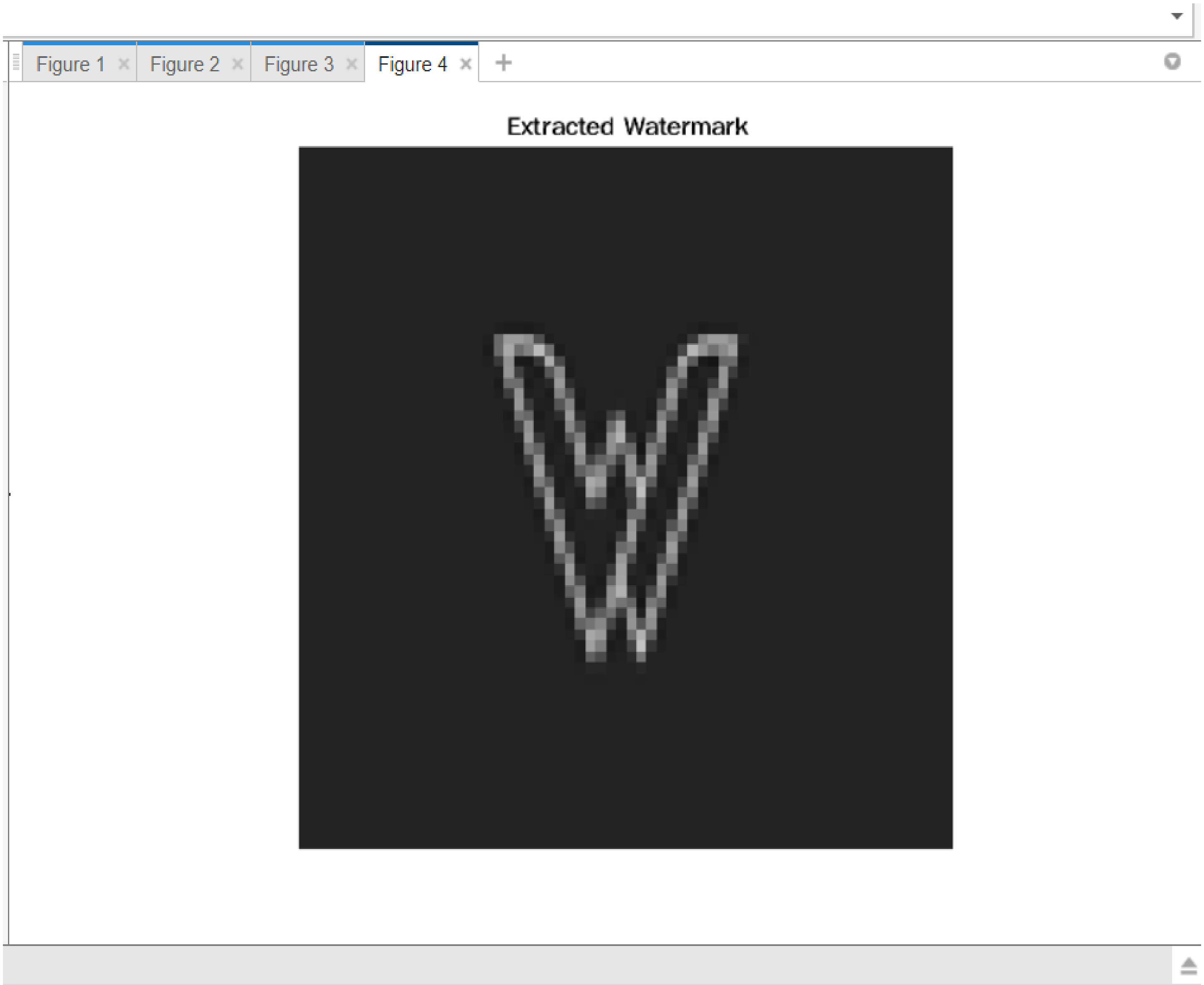


Fig 12 : Extracted Watermark

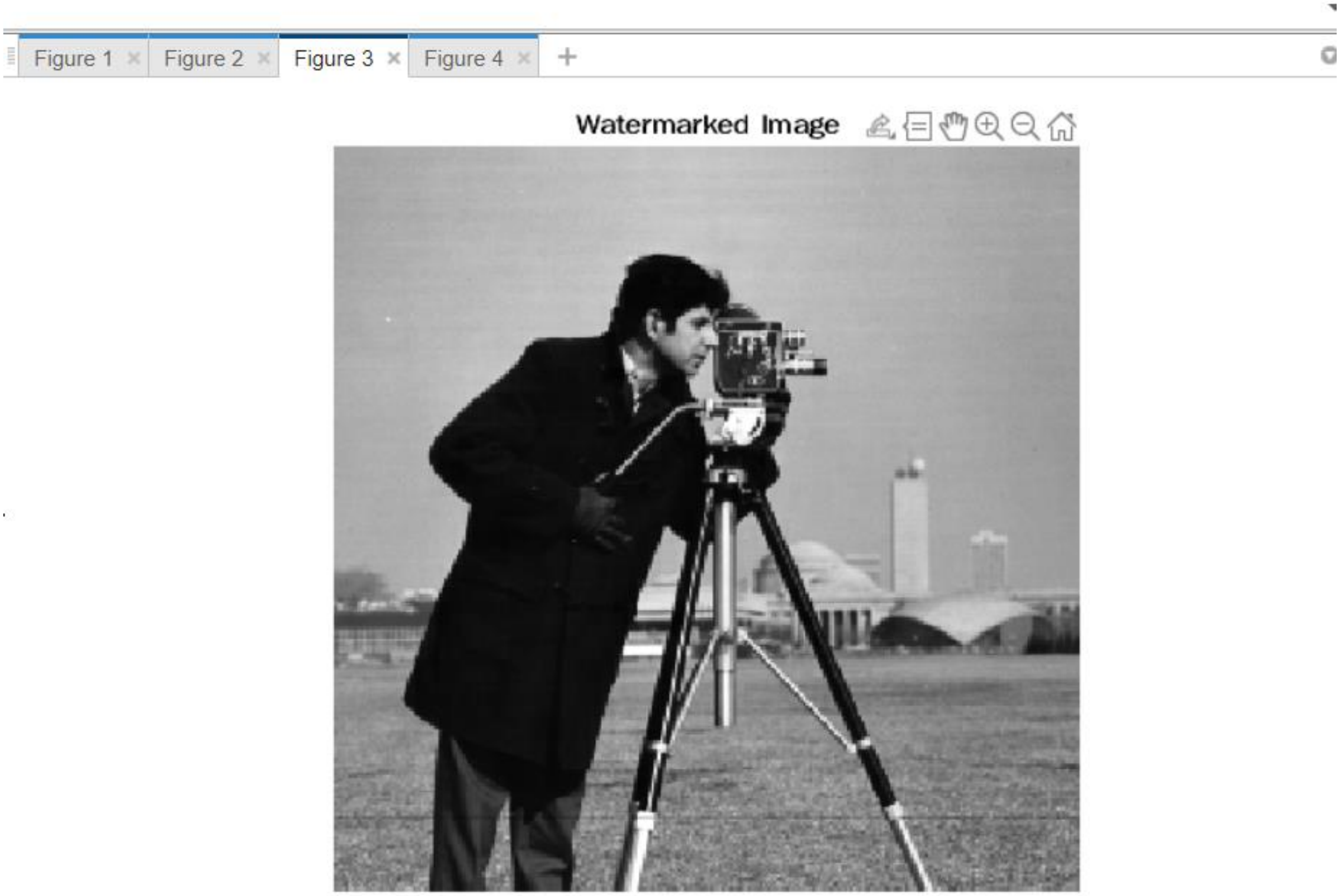


Fig 12: Watermarked Image

In figure 12 the output is of a watermarked image after doing the code on MATLAB . If any third party wants to copy the image then they will be exposed of owner validity authentication as the watermark (Fig 11) is already embedded in the original image.

Basically, Image watermarking is used to claim ownership of an image.

DISCUSSION –2.0

I demonstrated the watermarking code of MATLAB in an X-Ray of Apollo Hospital , so that the authentication remains with the respected hospital . Watermarking helps us to protect our images . We can add a visible watermark to your digital images and photos to protect intellectual property.

When organizations leave their digital assets unprotected, they can face serious implications, including asset misuse, brand depreciation, and legal fines. Additionally, with the number of resources being spent to create original content, plus the repercussions of misuse , to safe these important credentials And datas from third parties we must protect our data from getting surfaced across the board. Watermarking will basically Provides the real ownership of the raw data.

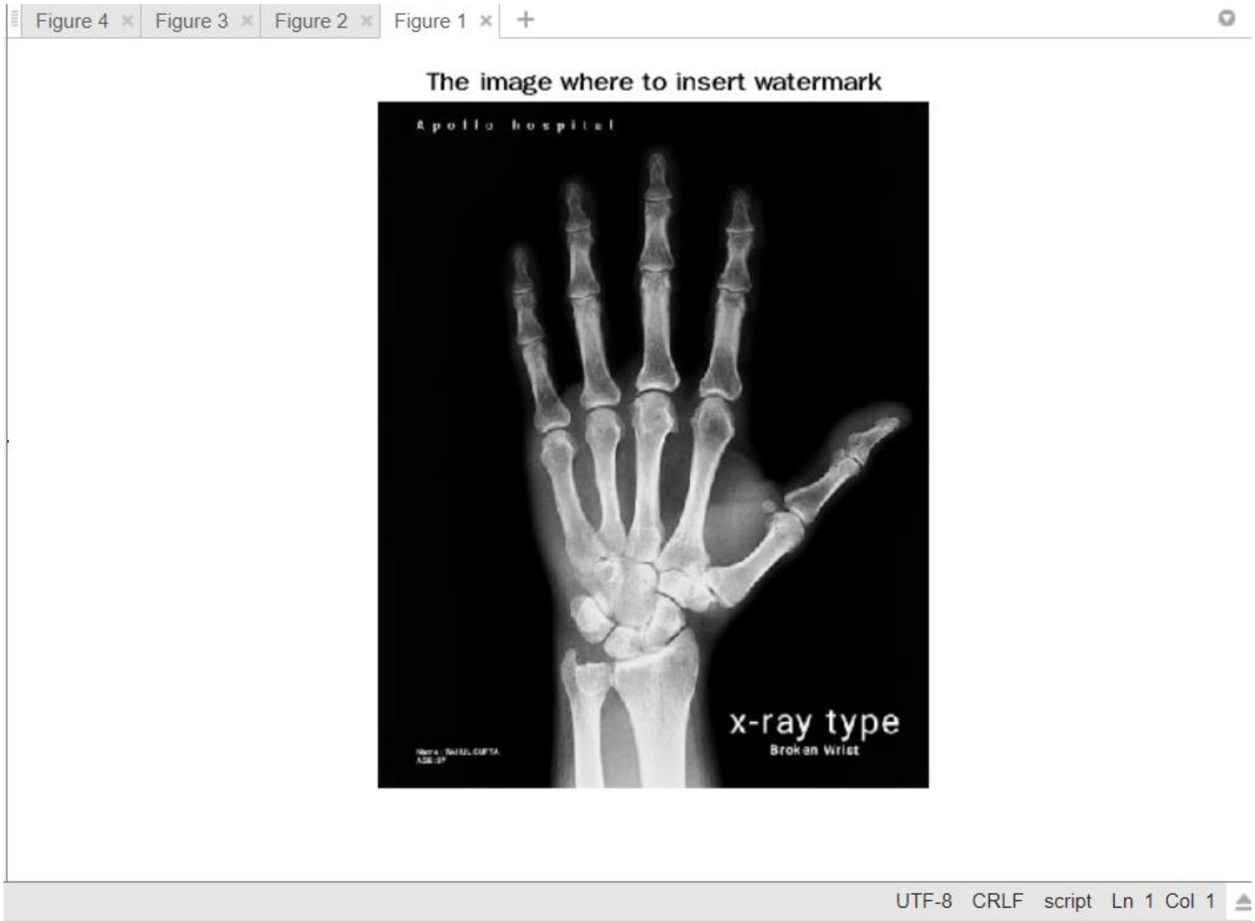


Fig 13 : The image where to insert watermark

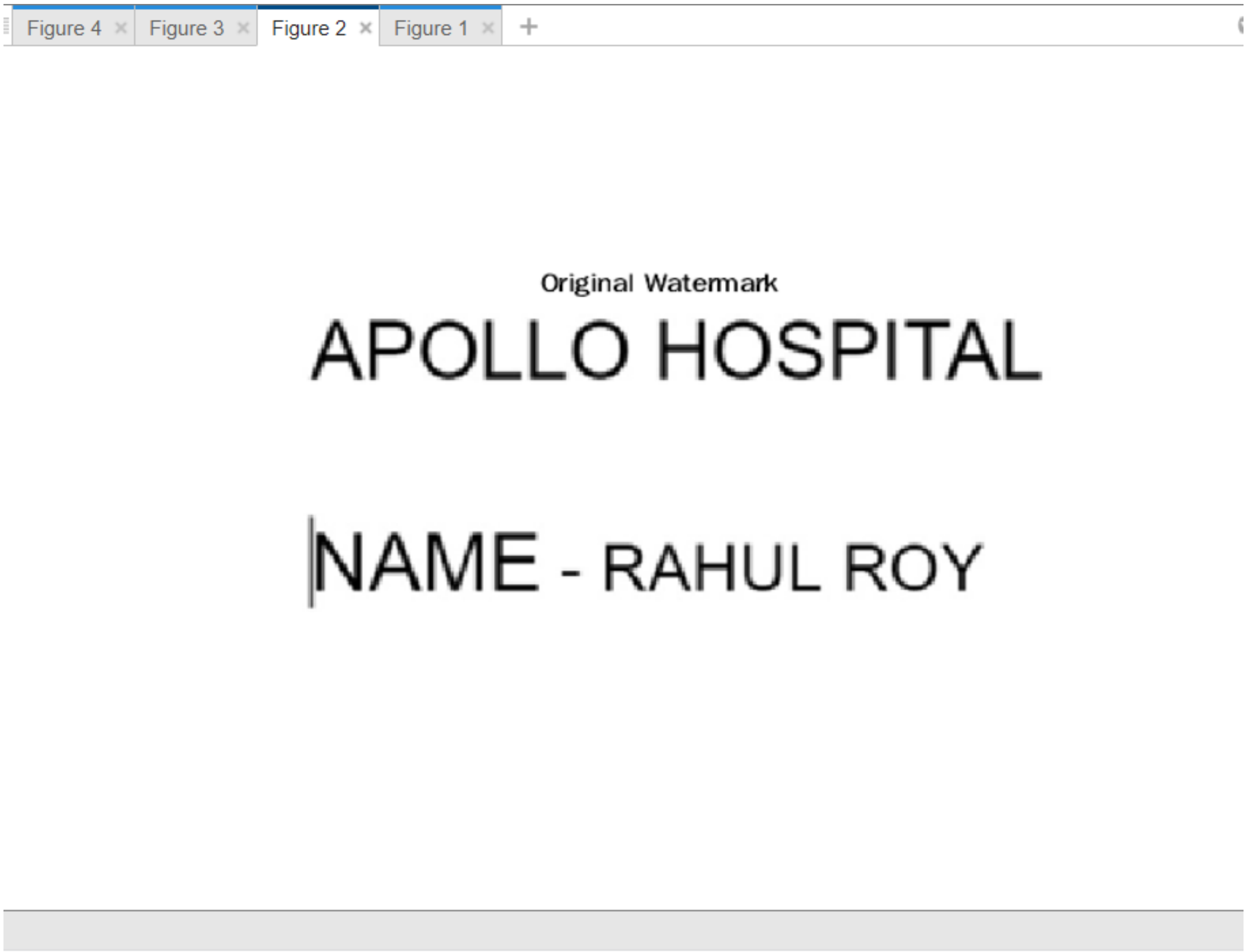


Fig 14 : original watermark

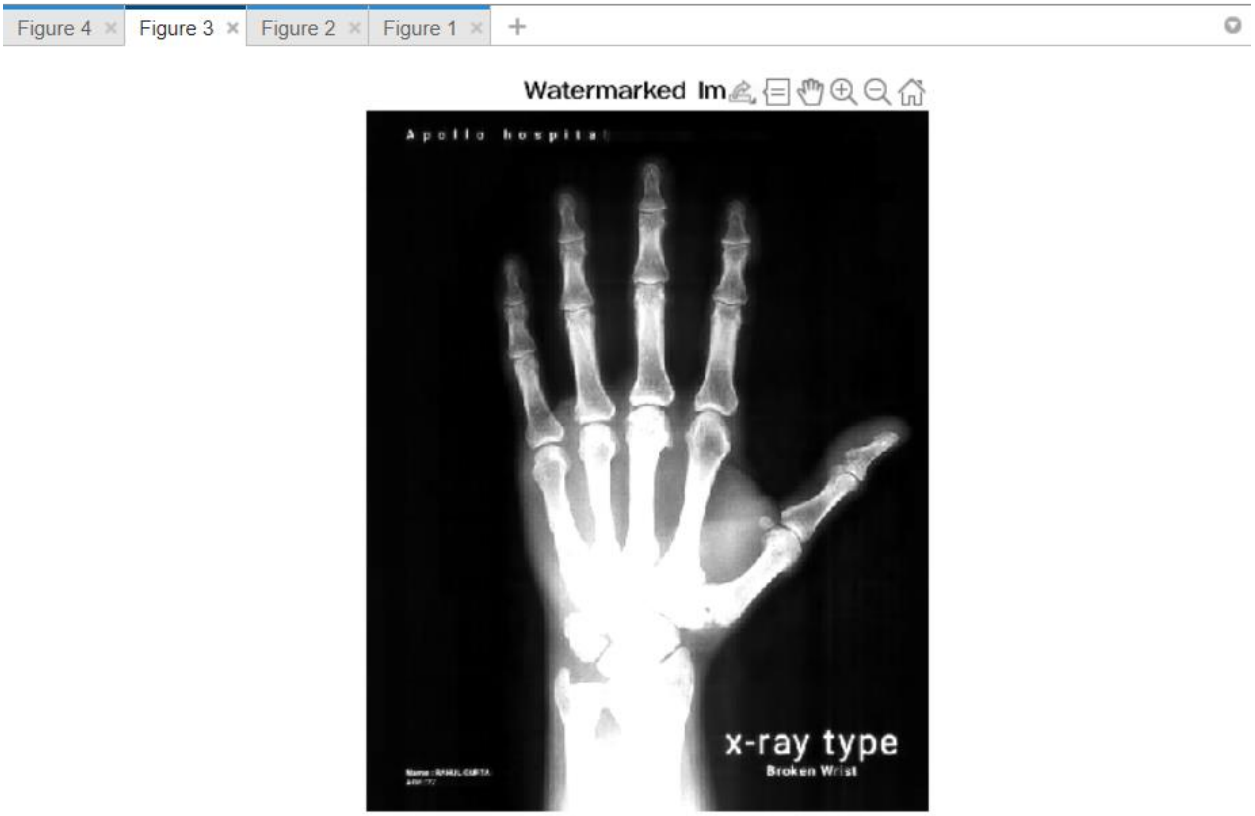
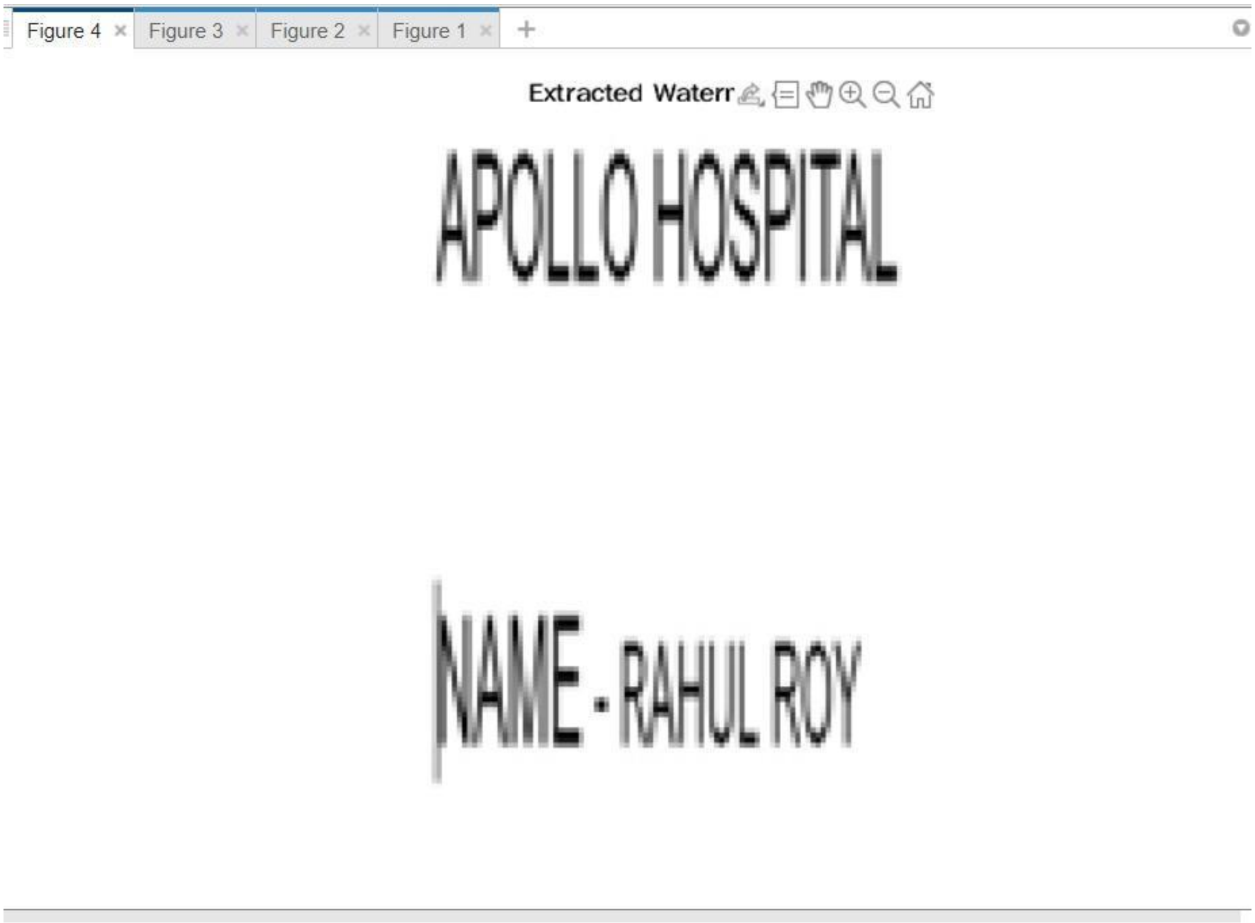


Fig 15 : watermarked image



APOLLO HOSPITAL

NAME - RAHUL ROY

Fig 16 : Extracted Watermark

CONCLUSION AND FUTURE DIRECTION

The field of digital watermarking is still evolving and is attracting a lot of research interest. The watermarking problem is inherently more difficult than the problem of encryption, since it is easier to execute a successful attack on a watermark. In cryptography, a successful attack often requires deciphering an enciphered message. In the case of digital watermarking, merely destroying the watermark, usually by slightly distorting the medium containing it, is a successful attack, even if one cannot decipher or detect any hidden message contained in the medium. The enormous popularity of the World Wide Web in the early 1990's demonstrated the commercial potential of offering multimedia resources through the digital networks. Since commercial interests seek to use the digital networks to offer digital media for profit, they have a strong interest in protecting their ownership rights.

Digital watermarking has been proposed as one way to protect such interests. Though much research remains before watermarking systems become robust and widely available, there is much promise that they will contribute significantly to the protection of proprietary interests of electronic media. Collateral technology will also be necessary to automate the process of authentication, non-reputable transmission and validation. An exhaustive list of watermarking applications is of course impossible. However, it is interesting to note the increasing interest in fragile watermarking technologies. Especially applications related to copy protection of bills with digital watermarks. Various companies have projects in this direction and solutions will soon be available. In addition to technological developments, marketing and business issues are extremely important and require in-depth analysis and strategic planning. It is very important to prepare the industry for the usage of digital watermarks and it is very likely that fully functioning to convince them of the added value their products can gain if they employ digital watermarking technologies.

REFERENCES

1.---https://alembicrarebooks.com/blogs/alembic-rare-books-blog/40160515-watermarks-foolscaps-exploring-the-history-of-paper-production

2.---https://www.researchgate.net/publication/357619320_Fusion_of_Watermarking_and_Steganography_for_Protecting_Image_Ownership

3.---https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.4.1641&rep=rep1&type=pdf

4.---http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.460.5149&rep=rep1&type=pdf

5.---https://link.springer.com/chapter/10.1007/978-3-319-12012-6_13

6—

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.84.-----5061&rep=rep1&type=pdf#:~:text=In%20watermarking%20terminology%2C%20an%20attack,is%20its%20robustness%20against%20attacks.

7.-----

https://towardsdatascience.com/understanding-singular-value-decomposition-and-its-application-in-data-science-388a54be95d?gi=2bfecb9d2fa0

8. YOUTUBE