Chapter 1

Introduction
CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION

Those amazing advancement about web need constructed the transmission, circulation and right will advanced networking thick, as advantageous (Ajish and Rajasree, 2014) Therefore, networking makers are additional every now and again managing particular illegal What's more unapproved utilization about their productions (Gupta and Raval, 2012) The thought about advanced watermarking originated dependent upon same time attempting to purpose the issues identified with the oversaw economy of scholarly advantages of networking.

Nowadays, Improvement for PC networks, conveyance for media results is turning into bit by bit additional normal and the issues about advanced copyright need turned an ever increasing amount renowned. So on, advanced watermark will be the new engineering in the field of copyright security. However it can't successfully measure those issue of the arithmetical attacks as far as image and the sway on the QR code quick examining qualities (Dolphin and Nancy, 2014).

In Recent years the common of the data which involves sound, image and video was kept in numeral system, Audiovisual data is digital form propositions several benefits and different abilities for normal user. Likely the most common used potential of digital media is the untroubled copy without degradation of the medium. Another convenience of digital multimedia is the ability of easy modification of its content (Cox and Miller, 1997). The above actions may be permissible, like the legitimate copy of a medical digital image for remote diagnosis purposes, or non-permissible, like the illegal copy and distribution of a digital music album.

In current session development about helter skelter pace PC networks also reality totally Web (WWW) need investigated method for new commercial, methodical, excitement also common chances for type of microelectronic distributed What's more advertising, massaging, ongoing data delivery, information sharing, coordinated effort "around computers, result ordering, transaction processing, advanced storehouses and libraries, web daily papers also magazines, organize feature What's more audio, personage correspondence. Furthermore parts that's only the tip of the iceberg. Those expense adequacy from claiming offering product in the manifestation about advanced images What's more feature successions by transmission over WWW will be significantly improved because of the change previously, innovation organization. We recognize that a standout amongst the greatest innovative occasions of the keep going two decades might have been the Attack of advanced networking previously, a whole extend about ordinary term
viewpoints. Advanced information could a chance to be saved effectively Furthermore with a helter skelter quality, furthermore it might a chance to be manipulated precise effortlessly utilizing workstations. Furthermore, advanced information could be transmitted clinched alongside a quick Furthermore modest best approach through information correspondence networks without losing nature.

Advanced networking offer a few dissimilar favorable circumstances in simple networking. The caliber about advanced audio, images and feature signs need aid higher over that from claiming their simple counterparts. Altering will be simple a result person might right the accurate discrete areas that necessity should a chance to be changed. Duplicating is straightforward for no misfortune from claiming devotion. A duplicate of an advanced networking will be indistinguishable twin of the unique. For advanced media circulation over globe totally Web, authentications are that's only the tip of the iceberg undermined over at any point because of the likelihood of boundless duplicating. The not difficult transmission What's more control of advanced information constitutes An genuine risk to majority of the data creators, and copyright managers need to a chance to be adjusted each time their fill in is utilized.

Furthermore, they need to make sure that their worth of effort may not be utilized within a shameful best approach (like Changed before advice). So, that advanced documents, copyright implementation also satisfied confirmation need aid exceptionally troublesome errands. Particular case result might a chance to be with limit right of the information utilizing a few encryption strategies. However, encryption doesn't give acceptable general insurance. When those encrypted information need aid decrypted, they camwood make uninhibitedly disseminated or manipulated.

One major issue may be identified with system advances What's more includes issues such as ‘web crawler’ and ‘pattern matching’ etc. Most important submissions include Rights founding, copyright and distribution control. Data hiding watermarks, also called steganography (Johnson 1999), are used to embed data in the images with the intention to have the data recovered perfectly at the receiver. Such methods usually assume that there are no hostile or even casual attacks. Error control coding is usually used to combat channel noise and casual signal processing. Major applications include secret communication over the internet and embedding of value added auxiliary data with such low economic values that there is no motivation for aggressive attack. 22

In today’s world we need to transfer confidential document, images from one place to another, so we need security to protect the data from the hackers hence visual cryptography is one of the most prominent approach to securely transmit data effectively and efficiently. But it
is not robust against various types of intentionally/unintentionally attacks from the hackers in transaction processing (Singh, Agarwal and Gupta, 2014). Hence, digital watermarking is best solution for providing more security to client/server shares in open communication channel during the transaction process. Now, in some existing methods only provide security against some normal attacks like Gaussian attack, jpeg attack, salt and pepper attack, etc. (Song, Sudirman, Merabti and Jones, 2010). But it is not robust against RST invariant attacks. So that we propose new approach for secure transaction of the data with two-way authentication scheme, hence we use 2-out-of-2 visual cryptography scheme with DWT (Discrete wavelet transform) based geometrically invariant image watermarking technique (Shi, Wang, Wen, Yue Wang, Huiping Zhao and Yanmin Yang, 2012).

![Diagram of watermarking process]

**Figure 1.1:** Rotation (R), Scale (S) and Translation (T) attacks in Network

To start new rapid contextual for watermarking, introduce the past in the documents hiding with associated terms. So on, further proceed onward will into discourse on the image watermarking system, prerequisites that watermarking framework must meet, sorts of the watermarking. Different attacks on a watermarking framework are as shown in Figure 1.1.

### 1.2 INTRODUCTION OF WATERMARKING

“More information is transmitted in a digital format now than ever, and the growth in this trend will not plateau in the foreseeable future. Digital information is susceptible to having copies made at the same quality as the original. There are many types of digital information and data. The types concentrated on in this report are:"

- Digital Images
- Digital Audio, and
- Digital Videos

“A watermark is a pattern of bits inserted into a digital image, audio or video file that identifies the file’s copyright information (author, rights, etc.). The name watermark is derived from the faintly visible marks imprinted on organizational stationery. Unlike printed watermarks, which are intended to be somewhat visible (like the very light compass stamp watermarking this report).
digital watermarks are designed to be completely invisible, or in the case of audio clips, inaudible."

In addition, the bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated. And finally, a digital watermark must be robust enough to survive changes to the file it’s embedded in, such as being saved using a loss compression algorithm e.g.: JPEG. Satisfying all these requirements is no easy feat, but there are a number of companies offering competing technologies. All of them work by making the watermark appear as noise - that is, random data that exists in most digital files anyway. Digital Watermarking works by concealing information within digital data, such that it cannot be detected without special software with the purpose of making sure the concealed data is present in all copies of the data that are made whether legally or otherwise, regardless of attempts to damage/remove it. The purpose of digital watermarks is to provide copyright protection for intellectual property that is in digital format.

Watermarking is the path toward hiding additional information inside programming codes, propelled data, (for instance, image, sound, and video) and reports to such an extent that it is about intangible. Progressed watermarking technique suggests the route toward embedding the given watermark information, (for instance, ownership information, name, logo, mark, etc. cetera,) in the guarded information, (for instance, image, sound, video, or substance) and option the given watermark information from the protective information, which isn’t seen by human perceptual structure.

By the day’s end, watermarking is a strategy of embedding an automated watermark or banner containing information fascinating to the copyright proprietor in the inquiry (content, image, sound, or video) which is ought to have been secured. An electronic watermark is described as an unmistakable or imperceptible conspicuous evidence code that is forever introduced in the data, to transmit covered data. It stays show in the data even after the deciphering methodology. It usually gives copyright confirmation of authorized development. The watermark is late used to recognize the truly copyright proprietor of the inquiry. Watermarking systems can be isolated into various types is as shown in the Figure 1.2 (Johnson and Katezenbeisser, 1999).

Rendering to the human view, the digital watermarks can be allocated into three different types as follows:

- Visible watermark
- Invisible Robust watermark
- Invisible Fragile watermark

Starting application view of understanding digital watermark might be
- Source based watermark
- Destination based watermark

**Figure 1.2: Types of Watermarking**

Source-based watermarks are alluring for proprietorship recognizable proof or verification where an exceptional watermark distinguishing the owner is acquainted with each one of the duplicates of specific programming being disseminated. A source-based watermark could be used for validation and to agree if got programming or other automatic information has been altered. The watermark should likewise be goal based where each dispersed duplicate gets a one of a kind watermark recognizing the specific purchaser. The aim based watermark could be used to follow the purchaser on version of illegal swapping.

**1.2.1 VISIBLE AND INVISIBLE WATERMARK**

The Visible watermark is a supplementary glowing covered into the essential programming codes. The watermark appears noticeable to an easygoing watcher on a cautious valuation. The undetectable watermark is put in such that variations made to the product codes are perceptually
not distinguished. The imperceptible delicate watermark is inserted such that any control or adjustment of the product codes would modify or obliterate the watermarks.

Image watermarking techniques can be classified into two broad categories: Spatial-domain based Watermarking and Transform domain based Watermarking as shown in Figure 1.3:

![Image Steganography Diagram]

**Figure 1.3: Image Steganography Techniques**

**Spatial (Time) Domain based Watermarking:**

In Time domain conspire, the mystery messages are implanted straightforwardly. Here, the most well-known and easiest Watermarking technique is the LSB addition strategy. In the LSB system, the minimum huge bits of the pixels are supplanted by the message bits which are permuted before implanting.

Most Watermarking programming shroud data by supplanting just the LSB of image with bits from the document that will be covered up. This strategy is by and large called LSB encoding. A standout amongst the most widely recognized systems utilized as a part of Watermarking.

Dong Zheng, Yan Liu, and Jiyong Zhao, 2006 briefly talked about the issue from claiming watermarking. Advanced images Likewise and only an all review on cryptography and advanced TV. Those. Writers furnished a depiction of a technique should embed a watermark under those minimum. Huge odds about pixels placed in the region about image forms. Since it depends ahead. Adjustments of the any rate as critical bits, the watermark will be undoubtedly wrecked. Further, their Technique is confined to images, in that it looks to embed those watermark under image areas. That lie on the edge from claiming forms.

Rhoads, 2003 portrayed a strategy that includes alternately subtracts little irregular amounts from every Pixel. Expansion or subtraction will be resolved toward contrasting a double masjid from claiming odds for the LSB of every pixel. On those LSB may be equivalent to those relating masjid bit, afterward those irregular. Amount will be added, overall it will be subtracted. Those watermark is subtracted by 1st. Registering those Contrast between those unique What's more
Chapter 1

Introduction

watermarked images et cetera by. Looking at those sign of the difference, pixel by pixel, should figure out whether it corresponds of the unique succession of additions what’s more subtractions. This strategy doesn’t aggravate utilization of Perceptual relevance, in any case it is recommended that the high back clamor be profiteered on. Give exactly heartiness on low pass sifting. This plan doesn’t think about the issue from claiming arrangement attacks.

**Patch Work Based Schemes:** Another, outstanding spatial space based plan is interwoven based strategy given by (Bender et al., 2011). They depicted two watermarking plans. The first is a factual technique called interwoven. Interwoven haphazardly picks sets of image focuses, and expands the brilliance at one point by one unit while correspondingly diminishing the splendor of another point. The second technique is called "surface square coding" where in pick up factor and IW the subsequent watermarked image.

Expanding k builds the strength of the watermark to the detriment of the nature of the watermarked image. To recover the watermark, a similar pseudo-irregular clamor generator calculation is seeded with a similar key, and the connection between the commotion design and potentially watermarked image is processed. On the off chance that the relationship surpasses a specific edge T, the watermark is identified, and a solitary piece is set. This strategy can without much of a stretch be reached out to a numerous piece watermark by isolating the image into squares and playing out the above method autonomously on each piece.

**Transform (Frequency) Domain Based Watermarking**

The transform domain Watermarking technique is used for hiding a large amount of data with high security, a good invisibility and no loss of secret message. The idea is to hide information in frequency domain by altering magnitude of all coefficients of cover image. It converts image blocks from spatial domain to frequency domain. Transform domain watermarking can be classified into following techniques is shown in Figure 1.4.

An advantage of the spatial techniques discussed above is that they can be easily applied to any image; regardless of subsequent processing (whether they survive this processing however is a different matter entirely). A possible disadvantage of spatial techniques is that they do not allow for the exploitation of this subsequent processing in order to increase the robustness of the watermark.

In addition to this, adaptive watermarking techniques are a bit more difficult in the spatial domain. Both the robustness and quality of the watermark could be improved if the properties of the cover image could similarly be exploited. For instance, it is generally preferable to hide watermarking information in noisy regions and edges of images, rather than in smoother regions.
The benefit is twofold: Degradation in smoother regions of an image is more noticeable to the HVS and becomes a prime target for loss compression schemes.

![Figure 1.4: Transform Domain Techniques](image)

1.2.2 DUAL WATERMARK

Dual watermark is a blend of an unmistakable and an imperceptible watermark (Cox I.J. and Matt L. et al, 2000). In this kind of watermark an imperceptible watermark is utilized as a reinforcement for the unmistakable watermark as is perfect from the Figure 1.5.

![Figure 1.5: Schematic Representation of Dual Watermarking](image)

1.2.3 ROBUST AND FRAGILE SOFTWARE WATERMARK

Robust watermarks can be removed regardless of whether they have been subjected to ill-disposed or easygoing semantics-saving or close semantics protecting code interpretation. Such watermarks are utilized as a part of frameworks that avert unapproved utilizations or counteractive action and in frameworks that influence open cases to programming possession (Cox, Kilian, Leighton and Shamon, 1996). Delicate software watermarks will dependably be demolished when the programming has been changed. Such watermarks are utilized as a part of uprightness check of programming and in frameworks that permit restricted change and duplicate.
1.3 TECHNICAL DETAILS

"Digital watermarking technology makes use of the fact that the human eye has only a limited ability to observe differences. Minor modifications in the color values of an image are subconsciously corrected by the eye, so that the observer does not notice any difference. While vendors of digital watermarking schemes do not publicly release the exact methods used to create their watermarks, they do admit for using the following basic procedure (with obvious variations and additions by each vendor)."

"A secret key (string or integer) produces a random number which determines the particular pixels, which will be protected by the watermarking. The watermark is embedded redundantly over the whole image, so that every part of the image is protected."

"One way of doing this is by "Patchwork". This technique uses a random number generator to select n pairs of pixels and slightly increases or decrease their luminosity (brightness level). Thus the contrast of this set is increased without any change in the average luminosity of the image. With suitable parameters, Patchwork even survives compression using JPEG. Although the amount of secret information has no direct impact on the visual fidelity of the image or the robustness of the watermark, it plays an important role in the security of the system. The key space, that is the range of all possible values of the secret information, x must be large enough to make exhaustive search attacks impossible."

1.4 WATERMARKING VS. STEGANOGRAPHY

"Watermarking is subsection of Steganography. In Steganography, abstracts which is hidden has no accord with the blind average and the claim from such an arrangement is that no suspicion should appear that an average is adapted any hidden data. In watermarking, nonmatching steganography, the abstracts which is hidden has accord with the blind average data. Abstracts hidden is the buying abstracts of the blind average and there is no affair like apprehensive that an accurate average is accustomed some absorb data."

"The determination of steganography is to receive a suppressed information among two parties i.e. actuality of the advice is unknown to an accessible attacker, and an acknowledged advance shall ascertain the actuality of this communication. On the contrary, watermarking, as connect to steganography, requires an arrangement to be watermark to oppose against attacks."

1.5 WATERMARKING VS. CRYPTOGRAPHY

"Cryptography can be defined as the processing of information into an unintelligible form known as encryption, for the purpose of secure transmission. Through the use of a key, the receiver can decode the encrypted message (the process known as decryption) to retrieve the original message. So, cryptography is about protecting the contents of the message. But as soon
as the data is decrypted, all the in-built security and data is ready to use. Cryptography scrambles a message so that it cannot be understood by unauthorized user. This does not happen in watermarking. Neither the cover medium nor the copyright data changes its meaning. Rather, copyright data is hidden to give the ownership information of the medium in which it is hidden."

1.6 WATERMARKING VS. DIGITAL SIGNATURE

The Digital signatures, similar accounting signatures, are acclimated to accommodate affidavit of the related input, typically alleged a message. Agenda signature is a cyber-banking signature that can be acclimated to accredit the character of the sender of a bulletin or the attest of a document, and feasibly to ensure that the aboriginal agreeable of the bulletin or certificate that has been beatific is unchanged. Agenda signatures are calmly portable, cannot be apish by addition else, and can be routinely time-stamped. The adeptness to ensure that the aboriginal active bulletin accustomed agency that the sender cannot calmly abandon it later. An agenda signature can be acclimated with any affectionate of message, whether it is encrypted or not, artlessly so that the receiver can be abiding of the sender's character and that the bulletin accustomed intact. An agenda signature is a far from the adequate message, admitting an agenda watermark is central asoftware message. Both, agenda signature and watermarking assure candor and actuality of a document. Agenda signature arrangement is accessible to baloney but a watermark arrangement has to abide a bound baloney level.

To decide Watermarking is including possession majority of the data previously, media substance will demonstrate the legitimacy. This engineering organization embeds an information, an inappreciable advanced code, in particular those watermark, resounding majority of the data something like those copyright status of the fill in to be secured. Constant endeavors would constantly constructed should gadget effective watermarking diagram Anyway systems suggested in this way don't appear to be will make strong will every one time permits attacks Furthermore media information transforming operations. The sudden demise build for watermarking premium may be well on the way because of those increment on worry again IPR. Today, advanced information security blankets such topics likewise get control, authentication, and Furthermore copyright insurance to even now images, audio, video. Furthermore media results. A buccaneer tries possibly to uproot watermark on abuse copyright alternately will cast those similar watermark, following adjusting the data, with fashion those evidence of legitimacy. Generally, those watermarking of even now images, video. Furthermore sound show sure normal key ideas.
1.7 APPLICATION AREAS OF DIGITAL WATERMARKING

A. DETECTION OF TEMPERING

"In this application area, it is necessary to assure that the origin of a data object is demonstrated and its integrity is proved. One example of temper detection is photographic forensic information which may be presented as evidence in the court. Given the ease with which digital images can be manipulated, there is a need to provide proof that an image has not been altered. Such a mechanism could be built into a digital camera (Cox I.J., Matt L. et al. 2000). For example, if a cop’s camera catches an over speeding vehicle then when proving the driver guilty in front of the judge, the accused may claim that the video presented in the court is tempered and the car shown in the video does not belong to him? A watermarking system which is embedded in digital cameras may help to resolve the issue. If somebody tries to temper the data, the watermark will get destroyed indicating that the data is tempered. In our country, a well-known example is the Tahalka-Scan.""

B. COPY PROTECTION

"Watermarking can be used as a strong tool to prevent illegal copying. For example, if an audio CD has a watermark embedded into it, then any of the system (Hardware like DVD, or software) cannot make a copy of it, and even if it copies, the watermark data will not get copied to new duplicate audio CD. Now the duplicate CD can be easily found because it does not have watermark data. Some schemes have attempted to satisfy more complex copy protection requirements. An early example is the Serial Copy Management System (SCMS), introduced in the 1980s, which enabled a user to make a single digital audio tape of a recording they had purchased but prevented the recording of further copies (i.e. second generation) from that first copy. The scheme failed ultimately because not all manufacturers of consumer equipment were prepared to implement the scheme in their products.""

C. COPYRIGHT PROTECTION

"The primary use of watermarking is where an organization wishes to assert its ownership of copyright for digital objects. This application is of great interest to big media organizations, and of some interest to other vendors of digital information, such as news and photo agencies. These applications require a minimal amount of information to be embedded, coupled with a high degree of resistance to signal modification (since they may be subjected to deliberate attack). For example, now a days, a news channel AAJ-TAK is showing the animal’s clips (which are already shown on Discovery Channel) by hiding the Discovery channel’s logo on the video clips. As per the law, The AAJ-TAK should show the courtesy sign and should pay the copyright fee to the
Discovery channel. In such cases, there is a strong need of watermarking as once the digital data is broadcasted, anybody else can start selling it without paying the IPR value to its owner.

D. ANNOTATION APPLICATIONS

"In this applications area, watermarks convey object-specific information (feature tags or captions) to users of the object. For example, patient identification data can be embedded into medical images. These applications require relatively large quantities of embedded data. While there is no need to protect against deliberate tampering. Normal use of the data object may involve such transformations as image cropping or scaling and will require the use of a technique that is resistant to those types of modification. For more details of various watermarking applications, one may refer."

E. FINGERPRINTING

"If monitoring and owner identification applications place the same watermark in all copies of the same content, it may create a problem. If out of n number of legal buyers of a content, one starts selling the contents illegally, it may be very difficult to catch who is redistributing the contents without permission. Allowing each copy distributed to be customized for each legal recipient can solve this problem. This capability allows a unique watermark to be embedded in each individual copy. Now, if the owner finds an illegal copy, he can find out who is selling his contents by finding the watermark which belongs to only singly legal buyer. This particular application area is known as fingerprinting. This is potentially valuable both as a deterrent to illegal use and as a technological aid to investigation."

F. BROADCAST MONITORING

"There are several types of organizations and individuals interested in monitoring the broadcast of their interest. For example, advertisers want to ensure that they receive the exact airtime that they have purchased from broadcasting firms. Musicians and actors want to ensure that they receive accurate royalty payments for broadcasts of their performances and copyright owners want to ensure that their property is not illegally rebroadcast by pirate stations. In 1997, a scandal broke out in Japan regarding television advertising. At least two stations had been routinely overbooking air time. Advertisers were paying for thousands of commercials that were never aired (Boland, Ruanaidh and Dautzenberg, 1995). The practice had remained largely undetected for over twenty years because there were no systems in place to monitor the actual broadcast of advertisements. This broadcast monitoring can be implemented by putting a unique watermark in each video or sound clip prior to broadcast. Automated monitoring stations can then receive broadcasts and look for these watermarks identifying when and where each clip appears."
1.8 TYPES OF WATERMARKING ATTACKS

Watermark attacks are classified into four distinct categories namely removal attacks, geometric attacks, cryptographic attacks, and protocol attacks, as shown in Figure 1.6.

![Diagram of watermarking attacks]

**Figure 1.6: Types of Attacks**

A. REMOVAL ATTACK

Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal (Singh, Agarwal, and Gupta, 2013).

B. CRYPTOGRAPHIC ATTACK

Cryptographic attacks deal with the cracking of the security. For example, finding the secret watermarking key using exhaustive brute force method is a cryptographic attack. Another example of this type of attack is the oracle attack (Singh, Agarwal, and Gupta, 2013). In the oracle attack, a non-watermarked object is created when a public watermark detector device is available. These attacks are similar to the attacks used in cryptography (Singh, Agarwal, and Gupta, 2013).

C. GEOMETRY ATTACK
All manipulations that affect the geometry of the image such as flipping, rotation, cropping, etc. should be detectable. A cropping attack from the right-hand side and the bottom of the image is an example of this attack (Singh, Agarwal and Gupta, 2013).

**D. PROTOCOL ATTACK**

The protocol attacks do neither aim at destroying the embedded information nor at disabling the detection of the embedded information (deactivation of the watermark). Rather than that, they take advantage of semantic deficits of the watermark’s implementation. Consequently, a robust watermark must not be invertible or to be copied. A copy attack, for example, would aim at copying a watermark from one media into another without knowledge of the secret key (Singh, Agarwal and Gupta, 2013).

Some other attacks are as under:

**A. INTERFERENCE ATTACK**

Interference attacks are those which add additional noise to the watermarked object. Lossy compression, quantization, collusion, demising, demodulation, averaging, and noise storm are some examples of this category of attacks.

**B. LOW PASS FILTERING ATTACK**

A low pass filtering is done over the watermarked image and it results in a difference map composed of noise.

**C. FORGERY ATTACK**

The forgery attacks that result in object insertion and deletion, scene background changes are all tantamount to substitution.

**D. SECURITY ATTACK**

In particular, if the watermarking algorithm is known, an attacker can further try to perform modifications to render the watermark invalid or to estimate and modify the watermark. In this case, we talk about an attack on security. The watermarking algorithm is considered secure if the embedded information cannot be destroyed, detected or forged.

**E. ACTIVE ATTACKS**

Here, the hacker tries deliberately to remove the watermark or simply make it undetectable. This is a big issue in copyright protection, fingerprinting or copy control for example (Singh, Agarwal and Gupta, 2013).

**F. PASSIVE ATTACKS**

In this case, the attacker is not trying to remove the watermark but simply attempting to determine if a given mark is present or not. (Cox et al 2002) suggest that, protection against passive attacks is of the utmost importance in covert communications where the simple
knowledge of the presence of watermark is often more than one want to grant (Singh, Agarwal and Gupta 2013).

G. COLLUSION ATTACKS

In collusion attacks, the goal of the hacker is the same as for the active attacks but the method is slightly different. In order to remove the watermark, the hacker uses several copies of the same data, containing each different watermark, to construct a new copy without any watermark. This is a problem in fingerprinting applications (e.g. in the film industry) but is not the widely spread because the attacker must have access to multiple copies of the same data and that the number needed can be pretty important (Singh, Agarwal and Gupta, 2013).

1.9 VISUAL CRYPTOGRAPHY SYSTEM (VCS)

Much visual information such as handwritten text, images is encrypted by visual cryptography. The encryption takes place in such a way that, to decrypt the secret, no mathematical computations are required. The original information that is to be encrypted referred as secret. Once the encryption is completed, ciphers are generated which is referred as shares. The part of secret in twisted form is known as share. To share the secret among group of n participants is the fundamental idea behind visual cryptography. The secret is divided into n number of pieces, referred as shares, in order to share the secret. After that, these shares are distributed among n participants. Each participant provides his own share, to reveal the original secret. If there is complete knowledge of only n-1 shares, then it is unable to decrypt the secret. There are many visual cryptographic schemes which are available, but the basic scheme is 2 out of 2 visual cryptography is as shown in Figure 1.7.

![Figure 1.7: Visual Cryptography Scheme](image)

The secret image has several schemes for encoding the pixels. Here, each pixel in the secret image is broken into four sub-pixels. A white pixel is shared into two identical blocks of four sub-pixels. A black pixel is shared into two complementary blocks of four sub-pixels. Figure
illustrates this scheme of encoding one pixel into four pixels in a \((2, 2)\) VC scheme. All the pixels in the original image are encrypted similarly using this scheme. These shares can be either Vertical or Horizontal or Diagonal Share as shown in the Figure 1.8.

![Figure 1.8: Pixel encoding in \((2, 2)\) Visual Cryptography scheme](image)

In this scheme the secret is divided into exactly two parts as shown in Figure 1.10 and Figure 1.11. These two shares must participate to reveal the secret. Another scheme in which the secret is divided into \(n\) shares and to reveal the secret any two shares must be participate in decryption process. This scheme is known as \(2\) out of \(n\) scheme as shown in Figure 1.12.

![Figure 1.9: Original Image](image)

![Figure 1.10: Visual encrypt image-1](image)

![Figure 1.11: Visual encrypt image-2](image)

![Figure 1.12: Combine visual encrypt image into Original image](image)

Third scheme of VC is \(K\) out of \(n\) scheme in which the secret is divided into exactly \(n\) parts. To reveal the secret any \(K\) shares are required. Multiple shares can be generated in visual
cryptography scheme. Another scheme which is extended version of third visual cryptography scheme, called n out of n, where secret is divided into n shares. All n shares must participate while revealing the secret.

1.10 WATERMARKING IN VISUAL CRYPTOGRAPHY

Watermarking is the technique of embedding a secret image into a host image without affecting its quality. Some process is used to reveal the secret image. The inseparability of the watermark (secret image) from the cover image is the significant advantage of watermarking. Hard to perceive, resists ordinary distortions, endures malevolent attacks, carries numerous bits of information, capable of coexisting with other markmarks, and demands little computation to insert and extract watermarks are some of the vital characteristics of watermark. To resist un-malicious or malicious attacks like scaling, cropping, lossy compression, and so forth, robust watermarking is used. There are different types of watermarking techniques. Based on the requirements for watermark extraction or detection, watermark can be divided into Non-blind, Semi-Blind and Blind schemes.

Phase 1: Visual Cryptographic Encryption

Phase 2: Hiding the shares using Digital Watermarking

Phase 3: Visual Cryptographic Decryption

The original image and secret keys are necessary for watermark detection in Non-blind watermarking scheme. The secret key(s) and the watermark bit sequence are required for extraction in Semi-blind scheme. Whereas, the Blind schemes require only the secret key(s) for extraction. Visible and Invisible are another categorization of watermarks based on the embedded data (watermark). A secondary image (the watermark) is embedded in a primary image in such that it is detectable to human observer in case of visible watermarking, whereas in case of invisible watermarking the embedded data is not detectable.

Here this scheme will add the merits of both visual cryptography as well as invisible and blind watermarking techniques. Here the secret shares are generated using basic visual cryptography model and then watermark these shares into some host image using invisible and blind watermarking. Because of this the secret shares are protected from cheating attacks. The decryption will be same as in the visual cryptographic model i.e. by stacking of the shares after the secret shares have been extracted by a simple watermark extraction technique.

1.11 IMAGE WATERMARKING CHARACTERISTICS

Following characteristics of an active watermarking system as below:

A. Robustness:
It is about the watermark summaries activity that the watermark extracts would not be damaged if accession achieves the accepted handlings with able to shocking attacks. The situation added of an acreage with additionally claim for watermarking and their account hang on the appliance region, “

B. Imperceptibility:

For watermarking, noiselessness activity which afterwards put in the watermark data, awning average would not adapt considerably. In added arguments, for attendance of Image watermark abstracts will not be affect the awning average actuality secure. If image watermarking arrangement should not be ensure for condition, it may appear that afterwards implanting image watermark summaries in an blind average (with image), messenger affection may adapt which the buyer of the angel resolve not ever like that a care device modifies his work.

C. Resilient to accept arresting processing:

“The watermark should be retrievable alike if accepted arresting processing operations are activated to the watermarked awning average data. These operations accommodate digital-to-analog and analog-to-digital about-face (i.e. demography the printout of an angel and again browse it to actualize accession agenda archetype of the image), re-sampling, re-quantization (including ambivalent and recompression), and accepted arresting enhancements such as angel contrast, accurateness and blush adjustment, or audio bass and acute adjustment, aerial canyon and low canyon filtering, histogram equalization of an angel and architecture about-face (BMP angel to JPEG image, MPEG cine to WMV movie, mp3 song to mp4 etc.).”

D. Fragility:

“Fragility agency that the watermark abstracts is adapted or abashed up to an assertive admeasurement back accession performs the accepted manipulations & awful attacks. Some appliance areas like atmosphere apprehension may crave a brittle watermark to apperceive that some about-face is done with his work. Some appliance may crave semi-fragility too. The semi-fragile watermark comprises a brittle watermark basic and an able-bodied watermark basic i.e semi-fragile watermarks are able-bodied to some attacks but brittle to others attacks.

E. Unambiguousness:

“Retrieval of the watermark should actually analyze the owner. Furthermore, the accurateness of buyer identification should not abase abundant in the case of an attack. The Unzign and Stirmark accept apparent arresting success in removing extracts anchored by commercially accessible programs. Watermarking of watermarked angel (re-watermarking) is additionally an above threat.”

F. Able-bodied to deception attacks (collusion and forgery):
“In addition, the watermark should be able-bodied to Bunco attack. Multiple individuals, who acquire a watermarked archetype of the data, may coast their watermark copies to abort the watermark attendance and can accomplish an alike of the aboriginal copy. Further, if an agenda watermark is to be acclimated in litigation, it charge be absurd for colluders to amalgamate their images to accomplish an altered accurate watermark.”

G. Resistant to accepted geometric alterations (image and video data):

“Watermarks in angel and video abstracts should additionally be allowed from geometric angel operations such as rotation, translation, agriculture and scaling. This acreage is not appropriate for audio watermarking.

1.12 STATEMENT OF THE PROBLEMS

There are many methods for watermarking type’s spatial domain and frequency domain, and it is used to protect information. Some of them are uses very complex methods which are very time consuming and some source information losses.

If someone is transmitting his private information by using watermarking technique, there are too much chances that the person lost private information because of any kind of external attack by some hacker or communication channel noise.

So here our main problem is to secure data in less time without affecting source information by making simple image processing algorithm.

![Image](image13.png)

**Figure 1.13:** Dual RST attacks

1.13 RESEARCH AIM AND OBJECTIVE

- To secure information using VCS and Watermarking.
- To Loss Less information based on Block DWT-SVD Transformation.
- To Recover Dual RST Attack Using Affine Transform with Pseudo Zernike moment and Surf features.
- To improve the PSNR and MSE value of Dual RST attacking Image Using Pseudo Zernike Moment.
• To hide the data based on alpha Bending Method.
• To verify the Information Based on QR-Code Technique.

1.14 SCOPE OF THE PROJECT AND WORK PLAN
• Secure and Fast Transmission of data over internet.
• Prevent against Online RST attacks.
• Less time and data Complexity.
• Easy and Fast way to recover data.
• Doesn’t Affect Cover image.
• Improve Recover data parameters PSNR and MSE.

1.15 NOVEL APPROACH ACCOMPLISHED
• Robust invisible watermarking based on DWT-SVD and Zernike moment.
• Prevent against Geometric Rotation, Scale and Translation attacks.
• Doesn’t affect for symmetric as well as non-symmetric rotation angles.
• Multi-layer Privacy based on QR-code, VCS and Watermarking.
• Improved PSNR, MSE, and Time and Embedding ratio.
• Works for Dual RST attacks.

1.16 STRUCTURE OF THE THESIS

The thesis is divided into six chapters; the following section is covering the short description of the chapters:

**Chapter 1:** Covers the introductory part to the driving forces of this work. This section covers objectives, scopes and novelty aspects of the research are detailed. Also, the methodology approach to fulfill the objectives is provided in the present chapter.

**Chapter 2:** This chapter is encouraged to know about the latest technology which is developed in Image Watermarking. It is also more focuses on the identifying the novel and innovative research for the enhancement of the performances. This chapter covers the problems related to Rotation, Scale and Translation attacks on Image Watermarking. Likewise this review of modern algorithms related to RST watermarking facilitates development in current year and innovative survey for forthcoming work.

**Chapter 3:** Presents the recent development and innovation in Gray image watermarking system. Also this chapter explores the depth review of gray image watermarking with Rotational, Scale and Translation attacks. However, this method emphasis on recent technology related to RST attack prevention Image watermarking system. It facilitates understanding of current scenario of Image watermarking relate to Combinational attacks. Review is not limited to individual
Chapter 1

Chapter 4: Describes the experimental set-up for the Color image watermarking system with dual RST attacks. For that we are describe the Block base methods with combination of Discrete wave late transform, Singular value Decomposing, Modified Pseudo Zernike moments and Affine Transform. This chapter also analyses Rotation attacks with translation-scaling in Combine or Separate manner and measure the PSNR and MSE values.

Chapter 5: Introducing a new concept of Non-Symmetric Rotation attacks. It means that whenever watermark image is rotated with different angle like 38°, 68° 94° or 188° etc. the data will be loss. This chapter covers image watermarking ability when perform the non-symmetric rotation angles and measuring the amount of losses occurs in terms of Peak Signal to Noise ration and Mean square Error. Also analyze the parameters with different graphs.

Chapter 6: In this Chapter presented Novel Approach using Region of Interest (ROI) watermarking. In that data is hided into the Cover image part so it will not tamper by any system. Chapter Covers analysis of Novel approach with different Symmetric and Non-Symmetric rotational attacks. This section also suggests further works and open doors to the researchers interested in this area.

Chapter 7: In this Chapter final conclusion of our work is presented as well as idea of future extension is described.