IJAER/July- August- 2021/Volume-10/Issue-1 ISSN: 2278-9677

International Journal of Arts & Education Research

A DETAILED ANALYSIS OF THE WATERMARKING OF DIGITAL IMAGES

PRAGYA DAKSH
Research scholar
Department of Computer Science
C.M.J. University Meghalaya

DR. AJAY AGARWAL
Supervisior
Department of Computer Science
C.M.J. University Meghalaya

ABSTRACT:-

As Web technology continues to advance at a rapid pace, the transmitter and movement of digital multimedia have become increasingly at risk. However, this development also has a negative side, in that it has resulted in an increase in dishonourable and illegal activities such as copying, modifying, falsifying, and infringing upon copyrights. This is a significant drawback of the development. As a consequence of this, the protection of intellectual property rights, the verification of material, and the identifying of ownership of media content have developed into essential requirements for watermarks. "The process of digital watermarking involves concealing a digital mark or logo, known as a digital watermark, within a multimedia signal in order to establish the authenticity of the owner at a later time. When producing watermarked media, a digital watermark is placed inside the source material to generate what is also known as signed media, watermarked signal, or simply watermarked media. After that, material that has been watermarked is used in combination with the original media or a key in order to extract the original watermark".

KEYWORDS:- Digital Images, Watermarking etc.

One of the viable solutions to the problem of unauthorised duplication, modification, and distribution of multimedia content is the use of digital watermarking. When using digital postprocessing, the image of the watermark is inserted directly into the cover picture. The clarity of the contained picture deteriorates as a result of the implantation of a mark inside the contained image. This mainstream press data is frequently dispersed in a format that is both condensed and encoded, and the postprocessing of these mainstream press data for the purpose of detecting copyright violations, providing evidence of ownership or authenticating media must sometimes be carried out in a realm that is both condensed and encoded. A system that manages facts in a format that is both condensed and encrypted is called "digital asset management" (DAM). When a

watermark is embedded into digital material, it has to be done so in such a manner that it can be identified for as long as the perceptual quality of the contents is at an appropriate level. On the internet, there is an absence of security, which means that photos may be duplicated and spread without the approval of their owners. In this kind of scenario, one of the methods for authenticating users, preventing copies from being made, and keeping track of rights to digital material is the use of watermarks. A digital picture is a class under electronic content. The durability of this approach is fully tested by extracting a one-of-a-kind watermark in an ideal manner, without causing any harm to the original picture. The "Digital Asset Management System (DAMS)" is responsible for managing information that is virtually condensed and encrypted. It is possible to use a watermark for the purpose of announcing ownership or exercising copyright protection on compression and encrypted material.

The reality that, in generally, encryption algorithms are employed extensively to increase the level of security provided by various signal processing applications served as the inspiration for the concept of organising and communicating planned activity. Image watermarking is a reducing computer vision application that genuinely addresses concerns about copyright violations and information authentication. This technology is concerned with the protection of intellectual property. As a consequence of this, techniques of encryption are regarded as the most appropriate instruments to boost the application's level of security. In addition to providing additional privacy transformation function, the Paillier cryptosystem is blazingly fast, which is essential for an SSP implementation. Image technique is recommended as a result of this finding as it is deemed appropriate.

1.2 Digital Media

Images, music, and video are only some of the several types of signals that may be found in digital media, along with data streams, time series, and symbolic sequences. On the other hand, for the sake of this thesis, we are only going to focus on photographs.

1.3 Imagesand Videos

A numerical representation of intensity values that are organised in a matrix constitutes a digital picture. These are made up of individual picture pixels. The brightness value of a single point represented by a (x, y) coordinate is denoted by each individual pixel. Using digital technology, it is possible to collect images, store them, and modify them. A bitmap is made up of an array of pixels in a rectangular format along its headers. Grayscale coloured and binary pictures are the two categories that describe it. A bitmap is

considered to be grayscale if the intensity values for each pixel fall anywhere between 0 and 255. On the other hand, a binary bitmap only has two possible values for each pixel, which are 0 and 1. If the intensity of each individual pixel can be expressed in terms of three bytes, then the picture bitmap in question is one that contains colours.

A series of still images is what people see when they watch a video. A common visual depiction of a video is seen in figure 1. It is attainable in both its uncompressed and compressed versions, depending on your preference. Video that has not been processed in any way before being saved is referred to as uncompressed video. Despite this, the quality of the uncompressed version is noticeably higher than that of the compressed version. However, there are problems with its storage capacity. This is especially the case due to the fact that uncompressed video formats have a significant memory need.

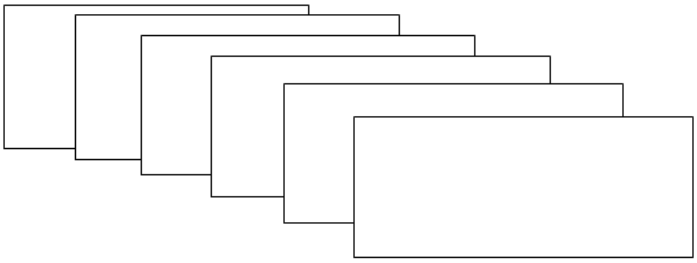

Figure 1.1*:* A video sequence

MPEG compression is often used when dealing with moving pictures or videos. In an MPEG-2 video device, there are descriptions of three different types of illustrative frames. The following descriptions apply to those frames:

- intraimageframesregularlycalledI-frames
- advancepredict frame calledP-frame
- bidirectionalframecalledB-frame

The I-frame is designed in such a way that it does not link to any other frames. The P-frame derives its movements from the I-frame or P-frame that came before it and can be utilized for extra predictions. B-frame video offers the highest possible grade of compressed and makes use of prediction in addition to the following I-frames or P-frames for movement correction. It is possible to predict a block in the sequence of frames by using a few distinct pieces from a previous region of space, from a future region of space, or by combining two blocks.

1.4 What is watermarking?

The process of embedding a message, phrase, logo, or autograph into a picture, audio file, movie, or any other kind of media is known as postprocessing. These customs have been around for quite some time—in fact, for many hundred years—and continue to this day. The practise of watermarks is still in its infancy, with the second part of the 1990s being the period in which it became more fashionable as a subject for academic investigation. The pictures that are used for watermarking may be made visible, as is the case with currency notes, or they can be ignored completely, in which case the watermark will be concealed inside the medium. The process of watermarking may be applied to real-world items; some examples of this include textiles, clothing tags, and packaging design. These items can be copyrighted with the use of specialised invisible stains and inks, as well as electrical signals. Some sorts of signals that may be watermarked include virtual version of audios, pictures, and videos. These types of media can all be stored electronically. The study for this thesis concentrates on embedding invisible watermark image utilising electrical signals as the medium. The watermarked job involves of an original medium that has not been watermarked and is known to as the covering or host medium. This medium may also be known to as the representative or transmission medium. In addition, the watermarked work contains concealed material (the watermark). A statement may be invisibly embedded in the host via a process known as watermarking. This can be accomplished through a variety of methods.

"It's possible to think of a watermarking system as a structure that's made up of two distinct components: an embedding component and a detecting component. The embedding stage requests two inputs from the user. The first thing is the message that we want to encode as a watermark, and the second thing is the host or cover work that we want to embed the mark in. The work will either be transferred or recorded after being watermarked. Using the detector, which identifies whether or not the watermark is there, one may decipher the hidden message that was placed in the file. The purpose of digital watermarking is to provide ownership security, which includes the identification of the copyright owner as well as protection. The overarching structure of the embedding and detection process is shown in Figure 2".

The following is a list of some generic words and meanings that are used in the field of watermarking:

“Watermark (noun)”: It is intended for the information that are given to remain secret. The verbs version of the word hallmark describes the method of embedding data, which is often analogous to a real watermark that is printed on paper.

The covering media is the media that either bears the stamp or hosts it. There are situations when the term "original media" or "host media" is employed.

"Watermarked data": The medium that has been imprinted with the watermark.

"Embedding": The method of incorporating the watermark into the primary media source.

"Extraction": The procedure that involves removing the encrypted message from the data that has been watermarked.

"Detection": The process that is carried out in order to determine whether or not a watermark is present on the medium in question.

"Watermarking": is the whole process, which includes embedding and extracting

Noise is any element in the signal that is not intended, such as one that may have been added when the signal was being sent or as a result of thermal processes.

"Attacked data": The data that has been watermarked and includes noise or inaccuracies as a result of artificial manipulation

1.4.1 "Types of watermarking data"

"The majority of the many ways for watermarking make use of logos or textual information as the watermark. There is also the possibility that watermarks are random numbers. Pseudo-random number generators, often known as PRN generators, are frequently used to produce these numbers. In the context of information security applications, PRN is employed rather often by researchers. Recent times have seen the usage of handwritten signatures. However, earlier systems were lacking in their comprehensiveness since they required the original picture in order to extract the watermark. Over the course of the last several years, many watermarking systems that may be used in combination with photographs taken by the cameras on mobile phones have been created. The systems that are being developed are for the purpose of protecting ownership and copyright. For the purpose of authenticating the present thesis, watermarks in the form of signatures and mobile phone numbers have been used. The typical watermark pictures that were utilised in the thesis are shown in Figure 2. When it comes to the signature, the binary integers that make up the signature are multiplied by either the 1D Walsh coding or the 2D Walsh coding. After that, the Walsh coded signature is

inserted into the DCT domain of the image's lower frequency band. When it comes to the mobile phone number, the size of the watermark is rather tiny in comparison to the host picture; hence, it is possible to embed it many times".

(a) Signature image (b) Mobile phone number

"Figure 1.2: The watermark images of signature image and mobile phone number"

In order to increase the resilience of the system against vertically cropping assaults, the decimals contact information are first transformed to binary digits and then randomized. After that, either a 1D or 2D Walsh coding is applied to the numbers. Likewise, the Walsh coded values are buried deep inside the Dct coefficients of the picture in the lower range of frequencies.

1.4.2 "Importance of watermarking"

The streaming of digital entertainment files has seen a substantial rise as a result of the widespread availability of desktop computers and the simplicity with which users may connect to the web. These digital files may consist of photographs, musical compositions, video recordings, or other types of information. In November of 1993, that the very first widely used internet browser was released, which marked the beginning of the Internet's transition toward a more user-friendly interface. The Internet is a great method for the dissemination of digital material due to the fact that it is economical, as well as the fact that it makes obtaining and sharing between enterprises and people quite straightforward. As a result, making copies of and making changes to these documents and records has become increasingly common. Concerns over the piracy of various forms of media have been voiced repeatedly over the course of many years. As a consequence of this, an immediate solution for the preservation of copyrights and authentication is required. The process of digitally embedding data such as logos, autographs, or texts into multimedia content such as photographs, videos, or music recordings is known as digital watermarking. This technique is an efficient method for protecting intellectual assets and copyrights. On the other hand, owners of content—particularly major Hollywood companies and record labels—perceive a significant threat posed by copying. In the past, utilising analogue devices carried a smaller danger than working with digital media does now; nonetheless, while it is possible to replicate an analogue file, the performance will suffer if you do so. On the other hand, due to the fact that digital media

voice recorders save data as a sequence of 1s and 0s, the quality of the music and movies that are created by using these devices is not affected in any way.

People are able to record and disseminate information that is subject to copyright protection by using electronic devices and attaching them to the internet. This does not return the information to the lawful content owners, nor does it compensate them for their work. Legal owners of property immediately began looking for an acceptable way to safeguard their legal interests. The use of cryptographic is perhaps the most widespread approach to the protection of digital material. And use this technology, items are encoded before they are sold, and the only individuals who have the cryptographic keys to completely view the file formats are the customers who purchased the encoded products. It is also possible to make the encrypted data accessible via the use of the web. Unfortunately, vendors are unable to supervise how a valid consumer treats the material once it has been decrypted in their possession. Once the hardcopy has been sold, it is possible for a pirates to acquire the product, use the private keys to access material that is not protected on subsequent copies, and then make many copies for the purpose of unlawful distribution.

Therefore, cryptography only offers a minimal level of security; once the consumer receives the encrypted text, there is no longer any security. Consequently, even after material has been encrypted, further security is still required. A potential technique that may be used to enforce the host's copyright laws is watermarking. Data is buried within the contents when using a digital watermarks. Attacks of all types, including as compressions, digital-to-analog conversions, as well as file format modifications, cannot defeat digitally watermarking. A watermark may be made to withstand each of these procedures. Several applications for copyrights protection as well as copy suppression have contemplated using watermarking. The watermark could be used to warn hardwares or software that copying must be prohibited in copy preventions. The watermark could be used in petitions for copyright protections to recognize the copyrights holder and guarantee correct payment of revenues. Watermarking has already been used or proposed for a variety of additional purposes, outside copy preventions and copyrights protection, that have been the main drivers of study in the topic. These consist of identification, broadcast surveillance, and transactions tracking. Medical photos, images from satellites, and photographs taken with mobile telephone cameras are among more applications that call for still picture watermarking.

As in watermarking procedure, a single secret key is often used. By detecting the watermarks, this private key is a crucial component in informing the user if the material is legitimate or not. Integration or embedding refers to the placement of the watermarking into the system. Exploitation or detection refers to the removal of

the watermarks. Using a watermarks is a strategy for copyrights protection as well as ownership confirmation since it increases the security and prevents tampering with digital data. There are several watermarking methods available. Every of them offers unique features and functionalities that may be used for various tasks. For instance, a delicate watermarking may be applied to digital content transferred over the internet for interference verification. The item is received on the recipient side. The embedded watermark would be removed to verify the content. If indeed the watermark cannot be removed, the content has likely been altered.

1.5 Watermarking properties

All watermarking method has a few very desired qualities that are extremely crucial. Depending on how the watermarking method is applied, some of these features are often in competition, and we are frequently compelled to make certain compromises between such properties. Performance is the 1st and maybe most significant characteristic. This is the likelihood that a watermarked picture's message would be successfully recognised. This probability should ideally be 1. The visual integrity is another crucial characteristic. The technique of watermarking modifies an original picture to add a message, hence it unavoidably degrades the picture's quality. So that no discernible variation in the picture's fidelity can be seen, we wish to limit this picture quality loss as little as possible. The packet size is the 3rd factor. Each work that has a watermark is utilised to convey a message. Because many systems need a somewhat large payload to be contained in a cover work, the quantity of such a messages is often crucial. Of fact, some applications just need the embedding of a single bits. Watermarking implementation of controls a lot of importance on the false positive rates. This is the percentage of digital files which are mistakenly labelled as having watermarks included when they do not. For watermarking devices, it should be maintained extremely low. And last, the majority of watermarking techniques depend on resilience. A watermarked composition may often be changed during the course of its existence, either via transmission above a lossy network or by several hostile operations that aim to erase the watermark or render it undetected. In addition to additive Gaussian noisy, compressing, printing, scans, rotations, resizing, cutting, as well as many other processes, a strong watermark must be able to endure them all.

1.5.1 Watermarking models

We may represent a watermarking procedure in a variety of ways. These may be roughly divided into one of two categories. Models are developed based on a communications-based perspective of watermarking are found in the 1st group, while models were based on such a geometric approach are found in the 2nd group.

1. **Communication-based models**

The classic concepts of communications networks are quite similar to how communications-based versions of watermarking are described. Actually, the procedure of watermarking involves sending a messages from the watermarking preserving towards the watermarking receivers. Therefore, it makes appropriate to represent this process using the secured communication concepts.

In a generic secured communication paradigm, the sender would be on one side and encrypt a message utilizing some sort of encoding keys to prevent listeners from decoding the messages if the connection was intercepted. When the message is then broadcast through a communication platform, more noise is added to the already noisy encoded messages. The receiver will then attempt to decode the noisy signal who used a decoding keys in order to recover the original messages after receiving it at another end of the transmissions. Figure 3 shows this procedure.

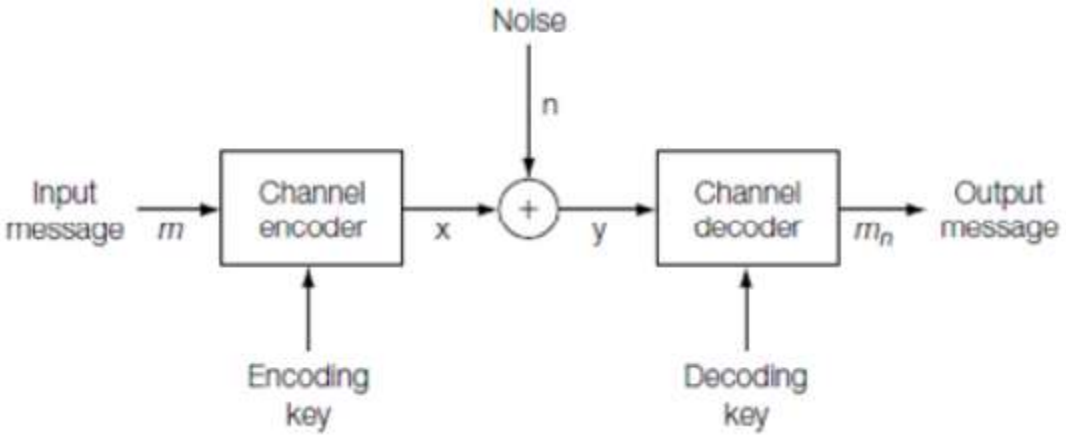

Figure 1.3: Standard model of a communications channel with key-based encoding

In generally, there are 2 sub-categories of communications-based watermarking methods. While the 2nd does not employ any side-informational at all, the 1st uses it to improve the watermarking processes. Any additional data that may be utilised to better encoded or decoded an input messages but isn't the message itself is referred to as side informations. The message's picture, which may also be utilised to give helpful information to improve the receiver's ability to recognise the signal, is the greatest illustration of this.

2. **Geometric models**

Thinking about watermarks in euclidean geometry is often helpful. Images, both watermarked as well as unwatermarked, may be seen as high-dimensional variables in this sort of paradigm, which is referred to it as the media world. Additionally, this is really a high-dimensional field that has all conceivable representations in all aspects. A 512 × 512 picture, for instance, might be expressed as a vectors with 262144 components in a 262144-dimensional region. In order to better visualise the watermarking processes utilising various areas depending on the desired watermarking features, geometric models may be quite helpful. One of these sections is the embedding zone, which would be the area that holds all the pictures that may be produced by inserting a messages using a watermarked embedding method into an unwatermarked picture. The detections zone, which contains all potential pictures through which a watermark may be effectively retrieved using a watermarked detection technique, is another crucial region. The zone of admissible fidelity, that includes all pictures produced by embedding a signal into such an unwatermarked picture that basically appears the same as the actual picture, is the last area to be considered. In order to create properly recognized watermarks which hardly affect picture quality, the embedding area for a specific watermarking systems must preferably sit within the convergence of the detection area and the zone of acceptable accuracy. Fig 5 depicts a geometric models as an illustration. The region of appropriate fidelity might be an n-dimensional realm centred just on authentic unwatermarked picture (co), with such a radius characterised by the greatest MSE we are prepared to accept for pictures with appropriate fidelity, as shown here. Mean square errors (MSE) is being used here as a metrics of fidelity. Depending on the criterion used to determine how an image contains an embedded watermarked or not, the detecting area for a detection technique based on vector correlation would've been specified as a half space. Keep in mind that the figure is only a 2D representation of an n-dimensional world.

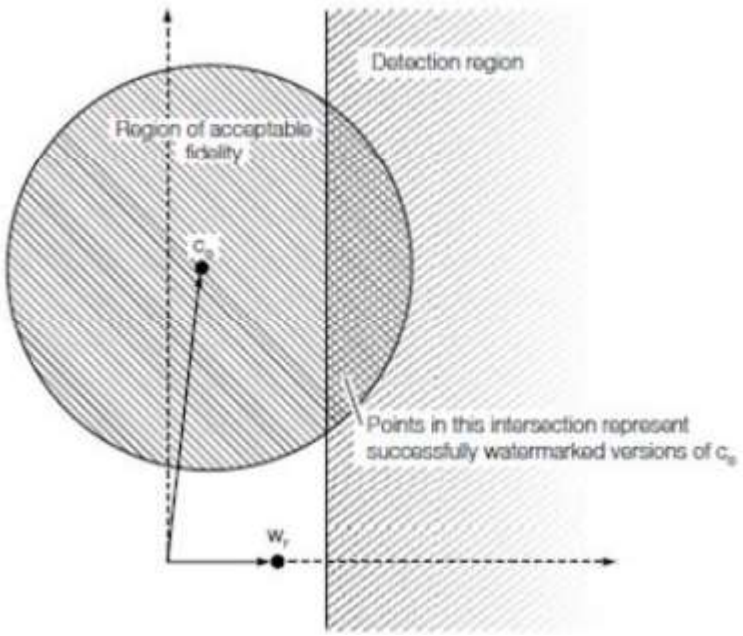

Figure 1.4 The region of acceptable fidelity (defined by MSE) and the detection region (Defined by linear correlation)

Occasionally it is more helpful to envision a projections of the news industry into a possible lower-dimension marked space, where the watermarking would then proceed as normal, while considering about sophisticated watermarking schemes. The reduced numbers of vector components makes this projection easier for computers to manage, consequently blocked-based watermarking methods, which divide pictures into blocks rather than working on a pixel based, may be able to represent this projections.

1.5.2 Image Watermarking Backgrounds and Frameworks

The fast development of international networked computers, the internet, plus multimedia applications has made it possible for digital information to be quickly disseminated across communications channels today. Digital picture watermarking enables the construction of a platforms for researchers by protecting digital material from unlawful ownership, copying, alteration, use, and dissemination via physical transmissions medium during communications, processing of information, as well as data management.

In order to enhance digitally watermarking processes, paper structure, grade, as well as quantity factors have been included, which dates back to 1282, when paper watermarks first appeared. Watermarking has indeed been widely utilised to improve security. Digital picture watermarking has seen several advancements since its introduction in 1988 as a computerised method that offers availability, secrecy, and integrity. An owners

authenticity indication (watermark) is inserted through into host image using watermarking methods, and the watermark data may subsequently be retrieved. A tiny bit, a collection of binary code, or even a variety of samples inside the host data might all be found in the watermarked data, which might or might not be visible. Info volatility is a key component of the digital picture watermarking strategy that mimics the human sensory perceptions systems. Information volatility may be used using a Just Noticeable Differences (JND) model to establish an ideal balance between imperceptibility, resilience, plus capacity of such a digital picture watermarking system. Information entropy may be described in terms of such masking effects, and it has the ability to decide where to enter the data. Such scenario provides improved robustness plus excellent imperceptibility while minimising perceptual distortion.The following concepts may be used to determine the volatility of an n-state systems:

Information Entropy,

$$ETP = -\sum_{i=1}^{n} P_i \log P_i$$

where $0 \leq P_i \leq 1$ and

$$\sum_{i=1}^{n} P_i = 1$$

where Pi denotes the probability of occurrence for the event i

A cover picture is the first step in the procedure for the protected transfer of a messages (host picture). The host picture may be seen as either pure noise, noisy with additional information, or a multimedia messages which has to be delivered. The communications path via which the watermarked information travels might be loud, lossy, or unstable. As a result, the collected signal might vary from the actual watermarked data due to potential assaults such as lossy compressions, geometric deformation, signal processing procedures, as well as signal conversions, among many others. A communications route over which a watermarked picture travels introduces noise. Such noise boosts information volatility, which raises the average amount of information in a picture that is unclear or ambiguous. Thus, particularly highly-resolution, complex-patterned pictures with a higher data entropy may be marked using watermarking methods. As a result, processing the encoded picture in a way that ensures a reliable image reconstruction is necessary to increase security. In a novel optical images encoding methodology, 2 deformable reflectors are used in lieu of the 2 random phases plates at the input as well as Fourier levels, accordingly, to produce the encoded picture using a random-phases encoding techniques in both planes. As just a result, the system is capable of achieving arbitrary beam bending in the image's amplitudes and phase parameters.

The digital picture watermarking procedure comprises of an embedding as well as an extraction step for a secured communication paradigm. The cover picture is 1st pre-processed in the watermarked embedding section, after which its unpredictability is assessed to determine the picture's integrating capability data. The encoder then applies an optical images encoding technique, employing a private key, to insert a watermark picture within the host image's high entropy value. The algorithm then obtains information on the phases and amplitude structuring of a laser light and produces the watermarked picture. Figure 5a shows the watermarked embedding portion. The watermarked picture is pre-processed before moving on to the watermarks extraction stage. The system then collects information on the phases and amplitude structuring of laser beam configurations. After that, these laser patterns' volatility is assessed. For the watermark extraction, a higher entropy ratio is used to offer higher resilience and interpretability. As shown in Figure 5b, a decoding uses the same key to extract the watermark information from the watermarked picture. The technology shows how easy, reliable, and undetectable it is to recreate the watermark picture from the original image.

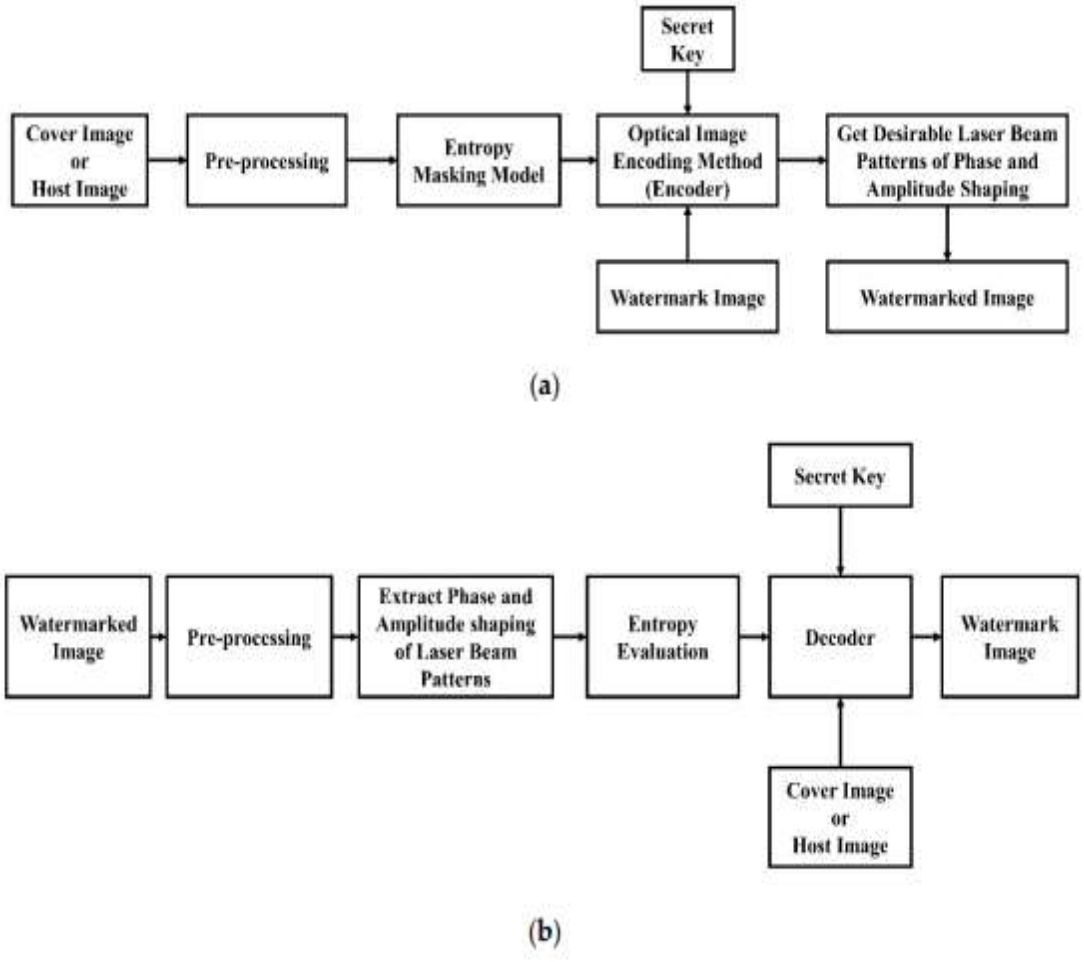

Figure 1.5 Watermark embedding and watermark extraction

A watermarked picture, DW, is created during the watermarked embedding procedure and may be characterised by the following functions:

$$Watermarked\ Image, D_W = E(I, ETP, W, K),$$

I is indeed the cover picture, ETP would be the informational volatility, W would be the watermark picture, while K is the safety key wherein E is the decoding technique. The watermark picture, W', which may be characterised by the accompanying decoder functions, is extracted during the watermarked extraction processes, where e(.) seems to be the decoding algorithms:

$$W' = e\left(D_{W,} K, ETP, I\right).$$

CONCLUSION:-

In the first section, we see a revealing connection suggested. Part 2 provides a clear analysis of the works that have influenced and guided the planned research. This third section compiles the mathematical designs of the numerous devices, methods, and evaluations used throughout the whole project. The experimental work is seen in fragment 4.

In this first part, we introduce the concept of watermarking with an eye towards a novel application. Even while we do mention watermarking's role in protecting various types of signs from access to open doors, the focus of this proposal is on watermarking compressed or blended images. Since watermarking compressed and blended images is necessary for a variety of uses, we've shown the strain techniques and encryption evaluations in a concise summary.

We present a detailed, consistent categorisation of watermarking strategies according to different perspectives, including watermarking location (spatial vs. repeated), watermarking visibility (obvious vs. hidden), watermarking strength (strong vs. subtle), watermark recovery methods (informed vs. randomly guessing), and watermark recovery locations (hard and delicate). As the quality of individual photographs is regularly fundamental, and as the regular place designs are especially vulnerable to picture administration assaults, we rapidly show the picture portrayal parts in the regular spaces. We have shown the DCT, DWT, LWT, and Contourlet transformations applicable here. In this concept, the Human Visual System (HVS) is assumed to play a crucial role in determining the maximum amount by which a coefficient may be modified by the application of a scaling factor. However, in the next sections, a favourable discussion and the

usefulness near the use of different HVS models especially valid for the suggested watermarking plans are presented. Finally, we take a look at watermarking's applications, paying close attention to how it works with compressed and composited images.

Part 2's survey of related making demonstrates that the experiment continues to focus on the field of automated watermarking, specifically on the organisation of plans suitable for both small-scale and variety pictures, which are more lenient against a wide degree of attacks while still being mindful of reasonable picture quality. Images like this may be shown with clinical and military data for further context. Almost all plans fail to assuage doubts, especially at extremes of image twisting or pressure. Non-obtrusive watermarking is prefered above both obvious and covert methods because it is necessary to hide the watermark or copyright information in the vast majority of instances. The most important option was deciding between weak and robust watermarking. It was decided to use energetic watermarking instead of passive ones since "Tamper ID" in media-advanced communication has more significant business concepts than the duplication or copyright control. Finally, it has been anticipated that the supervision of picture watermarking in the expanding universe, and more specifically the DCT and DWT-based shift towards developing areas of strength for a visually impaired picture watermarking strategy to mask a dubious watermark information, will be a necessary task. The decisions to be made also need to be accessible through a wide range of media materials, including compressed and uncompressed video information from the medical area.

REFERENCES:-

1. *Rajput, S., Ware, A., Umredkar, K., & Jeshwani, P. J. (2012). Digital Watermarking Using Machine Learning. International Journal for Research in Applied Science and Engineering Technology, 10(4), 2081–2085. https://doi.org/10.22214/ijraset.2012.40991*
2. *Rashid, A. (2016). Digital Watermarking Applications and Techniques:A Brief Review. International Journal of Computer Applications Technology and Research, 5(3), 147–150. https://doi.org/10.7753/ijcatr0503.1006*
3. *Saini, L. K., & Shrivastava, V. (2014). A Survey of Digital Watermarking Techniques and its Applications. 2(3), 70–73. http://arxiv.org/abs/1407.4735*
4. *Sen, J., Sen, A. M., Centre, C., & Hemachandran, K. (2012). an Algorithm for Digital Watermarking of Still Images. 3(1), 46–52.*
5. *Sharma, M., & Shiwani, S. (2013). Noise Attack Analysis on Non Blind DWT Watermarking Algorithm. International Journal of Emerging Technology and Advanced Engineering, 3(7), 374–378.*

6. Sharma, P. K. (2012). Analysis of Image Watermarking using Least Significant Bit Algorithm. International Journal of Information Sciences and Techniques, 2(4), 95–101. https://doi.org/10.5121/ijist.2012.2409

7. Sharma, R. K., & Decker, S. (2002). Practical challenges for digital watermarking applications. Eurasip Journal on Applied Signal Processing, 2, 133–139. https://doi.org/10.1155/s1110865702000574

8. Singh, T., & -, N. (2017). Digital Watermarking Using 2-DCT. International Journal of Engineering and Technology, 9(3S), 21–25. https://doi.org/10.21817/ijet/2017/v9i3/170903s004

9. Suhail, M. A. (2011). Digital Watermarking for Protection of Intellectual Property. Information Security and Ethics, 12(April), 8–12. https://doi.org/10.4018/9781599049373.ch265

10. Sur, S., Roy, R. G., Chakraborty, S., & Khan, A. (2015). Digital Watermarking: a Technical Overview. IOSR Journal of Electronics and Communication Engineering Ver. I, 10(4), 2278–2834. https://doi.org/10.9790/2834-10413438

11. Surajmal, M., Malik, V., Sangwan, N., Surajmal, M., & Sangwan, S. (2017). Digital Watermarking using DWT-SVD Algorithm. 10(7), 2161–2171.

12. Thapa, M. (2017). Digital Watermarking : Current Status and Key Issues. 327–332.

13. Tianhao Wang, F. K. (2019). ATTACKS ON DIGITAL WATERMARKS FOR DEEP NEURAL NETWORKS Tianhao Wang , Florian Kerschbaum University of Waterloo David R . Cheriton School of Computer Science Waterloo , Canada. ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2622–2626.

14. Tiwari, N. (2017). Digital Watermarking Applications, Parameter Measures and Techniques. IJCSNS International Journal of Computer Science and Network Security, 17(3), 184. http://paper.ijcsns.org/07_book/201703/20170322.pdf

15. Voloshynovskiy, S., Pereira, S., & Pun, T. (2001). Attacks on Digital Watermarks : Attacks , and Benchmarks. IEEE Communications Magazine, 8(1), 118–126.

16. Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J. J., & Su, J. K. (2001). Attacks on digital watermarks: Classification, estimation-based attacks, and benchmarks. IEEE Communications Magazine, 39(8), 118–125. https://doi.org/10.1109/35.940053

17. Wadhera, S., Kamra, D., Rajpal, A., Jain, A., & Jain, V. (2021). A comprehensive review on digital image watermarking. CEUR Workshop Proceedings, 2889, 126–143.

18. Wang, F. H., Pan, J. S., & Jain, L. C. (2009). Digital watermarking techniques. Studies in Computational Intelligence, 232(4), 11–26. https://doi.org/10.1007/978-3-642-03187-8_2

19. Yoo, I., Chang, H., Luo, X., Stava, O., Liu, C., Milanfar, P., & Yang, F. (2021). Deep 3D-to-2D Watermarking: Embedding Messages in 3D Meshes and Extracting Them from 2D Renderings. 10031–10040. http://arxiv.org/abs/2104.13450

20. Zhang, C., Wu, Y., Yu, Z., Li, Z., & Yao, J. (2017). Research and implementation of file security mechanisms based on file system filter driver. Proceedings - Annual Reliability and Maintainability Symposium, 154(Icmia), 174–183. https://doi.org/10.1109/RAM.2017.7889772

21. Zhong, X., & Shih, F. Y. (2019). A robust image watermarking system based on deep neural networks. ArXiv, 1–10.

22. Zotin, A. G., & Proskurin, A. V. (2021). Fast Implementation of Digital Watermarking Schemes Based on Arnold and Discrete Wavelet Transforms. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XLIV-2/W1-(April), 213–219. https://doi.org/10.5194/isprs-archives-xliv-2-w1-2021-213-2021