TECHNOLOGICAL PROTECTION MEASURES IN THE DIGITAL ERA: LEGAL ISSUES UNDER WIPO COPYRIGHT TREATY AND INDIAN COPYRIGHT REGIME

Sadaf Fahim[*]

I. INTRODUCTION

The WIPO Copyright Treaty (WCT) is a special agreement under the Berne Convention that deals with the protection of works and the rights of their authors in the digital environment. Any Contracting Party (even if it is not bound by the Berne Convention) must comply with the substantive provisions of the 1971 (Paris) Act of the Berne Convention for the Protection of Literary and Artistic Works (1886). Furthermore, the WCT mentions two subject matters to be protected by copyright:

> *(i) computer programs, whatever the mode or form of their expression; and*
> *(ii) compilations of data or other material ("databases"), in any form, which, by reason of the selection or arrangement of their contents, constitute intellectual creations. (Where a database does not constitute such a creation, it is outside the scope of this Treaty.)*

As to the rights granted to authors, apart from the rights recognized by the Berne Convention, the Treaty also grants:

(i) the right of distribution;
(ii) the right of rental; and
(iii) a broader right of communication to the public.

The right of distribution is the right to authorize the making available to the public of the original and copies of a work through sale or other transfer of ownership. The right of rental is the right to authorize commercial rental to the public of the original and copies of three kinds of works:

> *(i) computer programs (except where the computer program itself is not the essential object of the rental);*
> *(ii) cinematographic works (but only in cases where commercial rental has led to widespread copying of such works, materially impairing the exclusive right of reproduction); and*
> *(iii) works embodied in phonograms as determined in the national law of Contracting Parties (except for countries which, since April 15, 1994, have had a system in force for equitable remuneration of such rental).*

The right of communication to the public is the right to authorize any communication to the public, by wire or wireless means, including "the making available to the public of works in a way that the members of the public may access the work from a place and at a time

* Assistant Professor, Chanakya National Law University, Patna, Bihar, India.

individually chosen by them". The quoted expression covers, in particular, on-demand, interactive communication through the Internet[1].

The WCT is closely linked with the Berne Convention. Article 1(1) of the WCT provides that it is a special agreement within the meaning of article 20 of the Berne Convention. The preamble of the WCT supports this analysis. It stresses the necessity:

> *".....to maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information, as reflected in the Berne Convention"*[2].

The terminologies used under the WCT are similar to those of the Berne Convention. Article 13 TRIPS, when applied to limitation already complying with the special provisions of the Berne Convention and article 10(2) WCT, fulfills the function of additional safeguards. Hereby, the contracting parties may not fall short of the three-step test, the level of protection reached in Berne Convention.

Other than the Intellectual property treaties for its regulation, many organizations are not only promoting the awareness in intellectual property but also trying to strike the balance between the rights of the author under copyright and the right to qualitative education."[3] In this lengthy period, World Book and Copyright Day has won over a considerable number of people from every continent and all cultural backgrounds to the cause of books and copyright. It has enabled them to discover, make the most of and explore in greater depth a multitude of aspects of the publishing world: books as vectors of values and knowledge, and the depositories of the intangible heritage; books as windows onto the diversity of cultures and as tools for dialogue; books as sources of material wealth and copyrighted- protected works of creative artists. All of these aspects have been the subject of numerous awareness-raising and promotional initiatives that have had a genuine impact. There must nevertheless be no let-up in these efforts. Article 11 of WCT [4] talks about the works of an author as to who should be given their adequate legal protection and effective legal remedies in the exercise of their rights under Treaty or Berne Convention.

Article 12 of WCT deals with anti-circumvention regulation, it provides as[5]: It talks about the contracting states which are under obligation to provide legal remedies for any kind

---

[1] WIPO, WIPO Copyright Treaty, *available at:* http://www.wipo.int/ treaties/en/ip/ wppt/ summary_wppt.html (last visited on Nov. 21, 2024).

[2] *Ibid.*

[3] *See* WIPO Doc, CRNR/DC/4, Section 12.09. Moreover, it was raised in the course of the deliberations of Main Committee I. See WIPO Doc, CRNR/DC/102,72 and 74. Cf., as to the reference to the Berne Convention.

[4] *Supra* note 1, art. 11: Obligations concerning Technological Measures.
"Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."

[5] *Id*., art. 12: Obligations concerning Rights Management Information.
"(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:(i) to remove or alter any electronic rights management information without authority;(ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority."

of removal or alteration or of any of the above information as well as distribution of or communication to the public of copies of work with such removals or alterations. Article 12(2) of WCT, deals with Rights Management Information [6]: As, this section talks about the definition part, whereby it has been given how to recognise the author of the work and theirs rights when any of these items of information is attached to a copy of a work or any work of that sorts, communicated to the public.

II. TECHNOLOGICAL PROTECTION MEASURES (TPM)

A. Legal Aspects

TPM works to prevent copying. These are the measures that include a set of technologies like encryption, authentication, access control, digital watermarking, tamper-resistant hardware and software, and risk management architectures. In order to provide a secure distribution platform for digital content, DRM systems not only have to protect content against copying, but they must also offer means to identify and manage content.[7] In order to facilitate the automated trading of digital content and associated digital rights, DRM systems use so-called "metadata" to formally describe digital content and related parameters. With metadata, the content provider is able to control, in a very fine-grained manner, which consumer may access and use content, under what circumstances, and for what purpose. In particular, metadata enables the machine-readable identification and description of, content, content providers, and rights holders; usage rules under which content may be accessed and used; and of users of protected content. Such metadata may be stored in the special headers of a digital content format. It may also be embedded directly into the content with so-called "digital watermarking" technologies. With metadata, DRM systems are not only able to control access (who, for what purpose, and at what time), they can also control the geographical distribution of protected content.[8]

(Indian) Copyright Act, 1957: Section 65A of (Indian) Copyright (Amendment) Act, 2012[9] It talks about: The first clause of section 65A restricts the range of actions that may be considered circumvention to those applied for the protection of rights conferred by the

---

[6] *Id.*, art. 12(2): Rights Management Information.
"rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public."

[7] Peter K. YU, I *Intellectual Property and Information Wealth Issues and Practices in the Digital Age*, Copyright and Related Rights 323 (Praeger Publishers, 2007 edition).

[8] *Supra* note 3 at 327.

[9] (Indian) Copyright Act, 1957: (Section 65A of (Indian) Copyright Act, 2012) : (1)*"Any person who circumvents an "effective technological measure" applied for the purpose of protecting any of the rights conferred by this Act, with the intention of infringing such rights, shall be punishable with imprisonment which may extend to two years and shall also be liable to fine. (2) Nothing in sub-section (1) shall prevent any person from,- (a) doing anything referred to therein for a purpose not expressly prohibited by this Act: Provided that any person facilitating circumvention by another person of a technological measure for such a purpose shall maintain a complete record of such other person including his name, address and all relevant particulars necessary to identify him and the purpose for which he has been facilitated; or (b) doing anything necessary to conduct encryption research using a lawfully obtained encrypted copy; or (c) conducting any lawful investigation; or (d) doing anything necessary for the purpose of testing the security of a computer system or a computer network with the authorisation of its owner; or (e) operator; or (f) doing anything necessary to circumvent technological measures intended for identification or surveillance of a user; or (g) taking measures necessary in the interest of national security."*

Copyright Act. This provision cannot thus be extended to protect measures that purely restrict or control access to material outside of the protection conferred under the Act. Instead, it takes aim at the prevention of unauthorized copying, broadcasting, communication and the like. Section 65A envisages intention to infringe as a crucial element in the imposition of criminal sanctions. Under this provision, mere circumvention is insufficient without the intention to infringe the rights conferred by the Copyright Act. While this requirement is likely to increase the burden when prosecuting alleged offenders, it has the potential to shield 'innocent' or unintended acts of circumvention from criminal liability.

In contrast with the Digital Millennium Copyright Act (DMCA), the Indian Act does not criminalize the facilitation of circumvention either directly or through the production of tools which facilitate circumvention of TPMs. This omission—intentional or otherwise—would ensure that technological innovation is not adversely affected as has been the case in the United States where technologies for other purposes which only incidentally allow circumvention have been outlawed. Furthermore, under the proviso to section 65A(2)(a), no penalty is specified for a facilitator who does not maintain records of a circumvention. Is this the equivalent to the case of a person who actually circumvents the TPM? The Act provides no clear answer.

India and Copyright Act 1957:[10] Though India has not adopted WCT yet, it has amended the Copyright Act, 1957 by inserting *two parallel provisions* to this effect: Section 2 (xa) Rights Management Information Under Indian Copyright Law in 2012 [11]: as, this Section 2(xa), talks about, the author or performer's works and rights. Section 65 B: Protection Of Rights Management Information Under Indian Copyright Law In 2012 [12]: It talks about Section 65B, which deals with protection for RMI, which covers any information including the name of the performer, copyright information or an ISBN number which is used to identify or authenticate copies of a work or performance. The first clause of the section deals with the more direct offence of removing or altering RMI embedded in a work while the second clause of the section provides that anyone who, in an unauthorized manner, distributes, broadcasts, communicates to the public or otherwise markets copies of the work with the knowledge that RMI has been removed or altered is equally culpable as the person who removed it in the first place. The wording of this section is quite narrow and provides no exceptions such as those present in regard to TPMs. Problems that this approach could be faced with include instances of companies in converting copyright material into formats designed for (say) consumers with

[10] In USA, the Digital Millennium Copyright Act deals with this aspect but the difference being it makes it subject to certain exceptions: activities of law enforcement, intelligence or other authorized government agencies.

[11] "*Section 2(xa): Rights Management Information of (Indian) Copyright Act, 2012: (a) the title or other information identifying the work or performance; (b) the name of the author or performer; (c) the name and address of the owner of rights; (d) terms and conditions regarding the use of the rights; and (e) any number or code that represents the information referred to in sub-clauses (a) to (d), but does not include any device or procedure intended to identify the user."*

[12] *"Section 65B: Protection of Rights Management Information of (Indian) Copyright Act, 2012 : Any person, who knowingly,- (i) removes or alters any rights management information without authority, or (ii) distributes, imports for distribution, broadcasts or communicates to the public, without authority, copies of any work, or performance knowing that electronic rights management information has been removed or altered without authority, shall be punishable with imprisonment which may extend to two years and shall also be liable to fine: Provided that if the rights management information has been tampered with in any work, the owner of copyright in such work may also avail of civil remedies provided under Chapter XII against the persons indulging in such acts."*

disabilities—a concern voiced by Yahoo India in its submissions to the Parliamentary Standing Committee designated to look into the Bill's provisions.

Presence of copyrighted work in digital environment has become inevitable keeping in view following bundle of copyrights (exclusive rights) in a given work:

- *Right of reproduction*
- *Right of adaptation*
- *Right of distribution*
- *Right to communicate*
- *Right to use it in any medium*
- *Making derivative rights*

a) *It has made the reproduction, distribution and communication of works easier and within the competence of ordinary individual. New copies can be made with ease, speed and with absolute fidelity to the original and transmitted over vast distances and dispersed to millions of people in a few minutes or even seconds.*
b) *This has spread widespread unauthorized use and has increased piracy of copyrighted work materially affecting the economic interest of the owners.*
c) *So as to make USERS aware of whom work belong and under which system it has been protected, attempts are being made to secure work by displaying "certain information" surrounding the work as a „caution note" for the users or viewers or readers to use, read, view, or deal with it by keeping in view information surrounding the work. This is in the form of: „data identifying the information of the work". This data is classified as "Rights Management Information"*[13]
d) *This is being considered as suitable in the sense it helps in serving following purposes:*
    - *Proving ownership/authorship*
    - *Making a case of infringement*
    - *Displays information as to License, if any*
    - *Preventing users to deal with the work with restrictions (terms & conditions)*
    - *Allow consumers to rely on the accuracy of the information by creating a feeling of security in transacting online.*
    - *Confidentiality*
    - *Content integrity*
    - *Record of transaction*

Certain forms of RMI also collect information about users from their devices without their explicit consent: Section 65B, when read with section 2(xa), prohibits these forms of RMI. Such a definition ensures that consumer privacy is not compromised by the use of RMI. These issues aside, the question of whether criminal sanctions are warranted for an act potentially as 'docile' as removing or altering RMI—which primarily result in tangible, monetary losses—is one that is likely to remain uncomfortably unanswered. The amendments introduced through Copyright (Amendment) Act 2012 can be categorized into:

- *Amendments to rights in artistic works, cinematograph films and sound recordings.*
- *WCT and WPPT related amendment to rights*
- *Author-friendly amendments on mode of Assignment and Licenses*
- *Amendments facilitating Access to Works*
- *Strengthening enforcement and protecting against Internet piracy*

[13] *Ibid.*

- *Reform of Copyright Board and other minor amendments*[14]

B. Functional Aspects

(i) Access Controls

Access controls are measures that prevent someone from viewing, reading, hearing and/or otherwise perceiving the work without authorization from the right holder. Perhaps the most basic and frequently encountered form of access control is password protection, in order to get access to protected material. The passwords necessary to use the LexisNexis or Westlaw databases are examples of this type of protection. Also very common are IP address controls, which limit access to protected works to requests from specific computers or networks, common in the case of databases or software whose use is contractually limited to a particular campus, corporation, or other entity. For example, MovieLink is an online movie "rental" service that allows a user to download a movie to her computer for viewing, for a fee. She then has thirty days to watch the movie. However, once she begins watching it, she can access it only for twenty-four hours (after which the movie deletes itself from her hard drive).[15]

(ii) Use Controls

Use controls are technological measures that limit whether and to what extent a work can be copied, communicated, viewed or played. For example, technological controls often attached to motion pictures distributed on VHS tapes, usually referred to as "Macro vision", for the company that develops and markets the most commonly used form of such protection deters copying by affecting a substantial degradation of quality in any copy produced from the protected tape. The Serial Copy Management System (SCMS) is a use control measure that allows an unlimited number of first-generation copies (*i.e.*, "second-generation copies"). Use controls may also provide a usage function.

(iii) Protection for the Integrity and Authentication of Information

Technological controls can establish the authenticity of information, whether it comes from the source claimed and the integrity of the protected document, whether any alteration have been made, purposely or inadvertently. This information is valuable to all parties concerned: the recipient, the author, and the publisher. Even users who operate in an environment where payment for use is not a principal concern, for example, scholars and academics, value this function of protective technology.

(iv) Tracking

A distinct digital watermark can serve as a "fingerprint" that can provide an audit trail from which to trace an infringing copy to the original. While the technology does not prevent unauthorised copying, it can make it more detectable and assist in policing infringing uses. **Webcrawlers** are programs that methodically search the internet for copies of specified material and report where and when they were found. They are used by the recording industry

[14] *Ibid.*
[15] MovieLink, *available at*: http://www.movielink.com (last visited on May 20, 2025).

to detect unauthorized copies of sound recordings.[16] They are also used to track usage for licensing purposes. The "fingerprint" for which they search, however, need not be a watermark internal to the work. A digital fingerprint can be generated based on statistical measurements of a recording's sound.

III. TECHNOLOGICAL PROTECTION MEASURES (TPM) OF COPYRIGHT MATERIAL UNDER CYBERSPACE

A. Technical Aspects

Therefore, as Digital Rights Management (DRM), constitutes three important factors trough which it can protect the Copyright work, such as:[17]

a) *Digital Watermarking*
b) *Encryption*
c) *Biometric*

Now, question comes, what basically watermarks means and till what extent it is playing an important role in protecting authors rights?!

Fig. 1[18]: Watermarks

As, expressing the reasons, it might want to throw some light first upon, the importance of Watermarks.

(i) Watermarks

It is in the structure, picture, or content that is awed onto paper, which likewise gives proof of its credibility, whereby a recognizing imprint has been impressed on paper amid the course of production, which is very obvious or evident when paper is held up to the light. For instance: $ Bill. [19] In a closed system, *i.e*., one that requires special hardware or software to view a work, the watermark can serve as an integral part of an access or use control. For example, a mark could be inserted to permit the making of a certain number of copies (or first but not second-generation copies), after which the hardware would no longer make copies. Water-marks can also be used as part of a technological no longer make copies. Watermarks

[16] "RIAA Reveals Method to Madness", *Wired News*, Aug. 28, 2003, *available at*: http://www.wired.com/news/digiwood/0,1412,60222,00.html (last visited on May 23, 2025).
[17] M. Swanson, B. Zhu, *et.al.*, "Robust audio watermarking using perceptual masking" 66 *Signal Processing:* Special Issue on Watermarking, 337-347 (1997).
[18] *Ibid.*
[19] *Ibid.*

can also be used as part of a technological screening device to prevent recording or playback of works that have been copied or compressed without authorization in such a system. This concept underlay the dormant (and apparently defunct) Secure Digital Music Initiative (SDMI).

(ii) Encryption

Encryption is a method of disguising or encoding information so that only certain users can remove the code and view the information in its original, non-encrypted form. A system of encryption is based on an algorithm, or formulas. A very basic algorithm might be "shift by n," where each letter used in the message is shifted n spaces (where n is a number from one to twenty–five corresponding to the positions of the remaining letters of the alphabet). For example, if the encryption key is n=3, the encrypted version of MEET TONIGHT IN PARK would be PHHWWRQLJKW LQ SDUN**.** This simple shifting cipher would never be an adequate encryption method because the set of all possible keys is too small. It would not take a computer (or a human being, for that matter) very long to try each of the twenty-five possible letter shifts and stop at the right key when it found recognizable text. Obviously, the larger the possible number of keys, the more powerful the encryption. One more robust method is called a one-time pad and uses a key that is the same length as the clear text. A digital file that is represented by a ten-digit series of 1's and 0's would have a key that was also ten digits long and would result in a ten-digit ciphertext. The problem with a longer key is that it makes the encryption and decryption process slower. "Pretty Good Privacy" (PGP), *is one of the best software and it's a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication.*

(iii) The DeCSS Case

Content Scramble System (CSS) is an encryption scheme to protect movies on DVDs. It can be decrypted in DVD players with a set of 'player keys' with understanding of the CSS encryption algorithm. Without the player keys and the algorithm, a DVD player cannot access the content of a DVD. A DVD player can display the movie on television or a computer screen with the player keys and the algorithm, but it cannot copy it on a computer or manipulate its content. This technology was licensed to the manufacturers of DVD players who were obliged to keep player keys confidential. Linux is an operating system. In 1999, it did not support any DVD player. Jon Johansen, a 15-year-old Norwegian teenager, wanted to develop a DVD player in Linux. In September 1999, he reverses engineered licensed DVD player and found out the player keys and other information necessary to decrypt CSS. He wrote a decryption program called DeCSS. This program can decrypt the DVD's CSS protection. It allows the user to copy the DVD files and place on their hard drive.

The Motion Picture Association of America (MPAA) requested the Norwegian Economic Crime Unit to start criminal proceeding against Johansen for unscrambling CSS and writing DeCSS. Johansen was charged with violating the Norwegian Criminal Code, section 145(2), which outlaws breaking into another person have locked property to gain access to data that no one is entitled to access. This was for the first time that the Norwegian Government had attempted to punish the individuals for accessing their own property. Previously, the Government had used these laws to prosecute only individuals who had violated someone else's secure system, like a bank or telephone company system, to obtain another person's records. The three-member Oslo City Court unanimously acquitted Johansen. The court found that Johansen was entitled to access information on a DVD that he had purchased, and was,

therefore, entitled to use his program to break the code. The appeal filed by the Government was also dismissed.[20]

B. Information Hiding Techniques

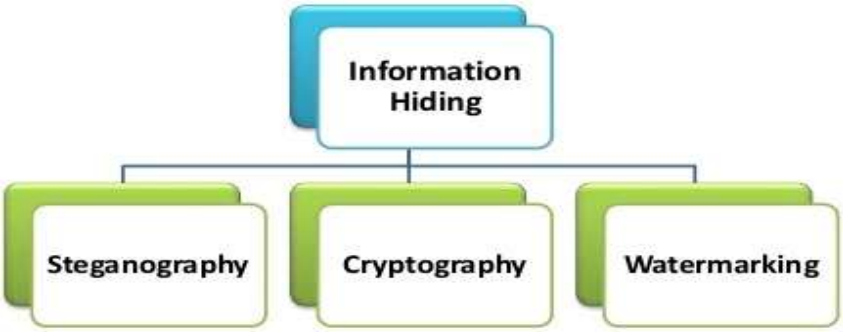


Fig.2[21]: Information Hiding Techniques

Along these lines, Digital watermarking is an expansion of watermarking idea in the computerized world as advanced watermark is an example of bits embedded into a computerized picture, sound or feature record recognizes the document's copyright data (author, rights, etc.)

(i) Attacks[22]

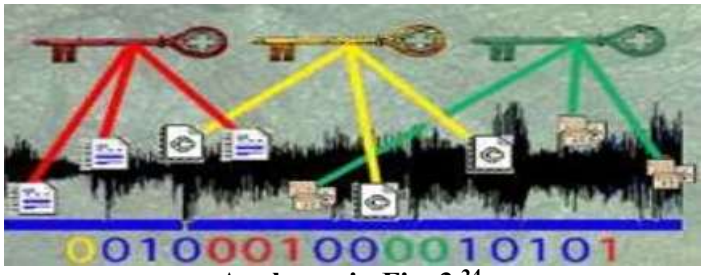
Attacks on watermark may not so much evacuate the watermark, yet incapacitate its readability. Image preparing and changes are ordinarily utilized to make and apply watermarks. These same methods can likewise be utilized to debilitate or overwrite watermarks. Multiple watermarks can be put in a picture and one can't figure out which one is substantial. At present watermark enlistment administration is "first come, initially served." Someone other than the legitimate holder may endeavour to enrol a copyright first.

Types Of Attacks On Watermarks:[23]

a. Removal attacks
b. Geometrical attacks
c. Cryptographic attacks
d. Protocol attacks, which talks about the types of watermark, namely:
   - *Robust Watermark:* A robust watermark is a watermark that is difficult to remove from the object in which it is embedded.
   - *Fragile Watermark*: A fragile watermark is destroyed if anybody attempts to tamper with the object in which it is embedded.
   - *Visible Watermark:* A visible watermark is immediately perceptible and clearly identifies the cover object as copyright-protected material, much like the copyright symbols ã, â, and ä

[20] Justice Yatindra Singh, *Cyber Laws* 52 (Universal Law Publishing Co. Pvt. Ltd., 5th edn.).
[21] L. Boney, A. Tewfik, *et.al.*, "Digital watermarks for audio signals" in IEEE Proc. Multimedia, 473-480 (1996).
[22] *Ibid.*
[23] *Supra* note 15 at 339.

- *Invisible Watermark*: An invisible watermark is not normally perceptible, but can still be used by the rightful owner as evidence of data authenticity in a court of law.
- *Public & Private Watermarking*: Public Watermarking Users of content are authorized to detect watermark, whereas, Private Watermarking Users not authorized to detect watermark
- *Asymmetric & Asymmetric Watermarking:* Different keys used for embedding and detecting watermark, whereas, Symmetric watermarking. In symmetric watermarking same keys are used for embedding and detecting watermarks.



As shown in Fig. 3.[24]

- *Steganographic & Non-Steganographic*: User aware of the presence of a watermark. e.g.: - User to detect piracy. Steganographic Watermarking User unaware of the presence of a watermark e.g.: - Used in fingerprinting applications, whereas Non-Steganographic Watermarking, used when the user is aware of the presence of a watermark. e.g.: - User to detect piracy.

Important Parameters:[25]

- Transparency
- Robustness
- Security
- Capacity
- Invertibility (reversibility)
- Complexity
- Possibility of verification

Common watermarking techniques:[26]
Choice of Watermark Object

- Time domain-LSB Modification
- Frequency Domain
- Wavelet Domain

Presently, essentially how Watermarking is through and through not quite the same as Steganography and Cryptography: the fundamental reason for steganography is only to shroud a message m in some sound or video (cover) information ***d***, by individuals, in such structures that an eavesdropper cannot recognize the vicinity of ***m*** in ***d'***. Thus, the fundamental objective

[24] Keshav S Rawat, Dheerendra S Tomar, "Digital watermarking schemes for authorization Against copying or piracy of color images" in IEEE, Vol. 1 No. 4, 295-300.
[25] *Supra* note 20.
[26] *Ibid.*

of watermarking is to conceal a message m in some sound or feature (spread) information ***d,*** to acquire new information ***d'***, essentially vague from ***d***, by individuals, in such a route, to the point that a eavesdropper can't ready to either evacuate or supplant in ***d'***.
Presently, clarifying the distinction between **Cryptography and Watermarking**:[27]

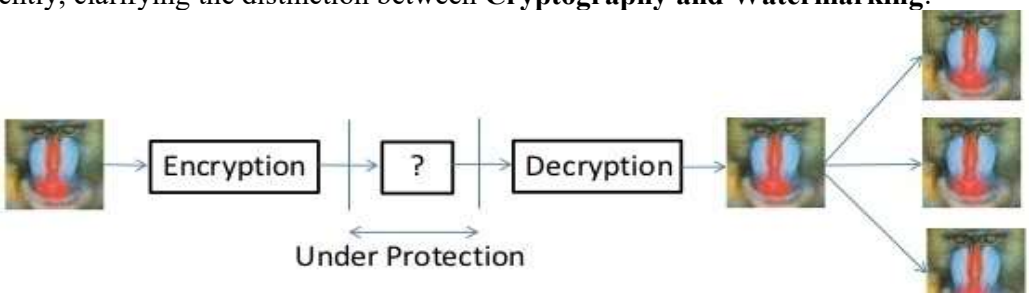


Fig.4[28]: Digital Watermarking

Cryptography is the most widely recognized method for ensuring advanced substance and is one of the best science as created till now. On the other hand, encryption can't help the seller to screen how a legitimate customer handles the substance or content after decryption as Digital watermarking can secure substance or content even after it is decrypted.

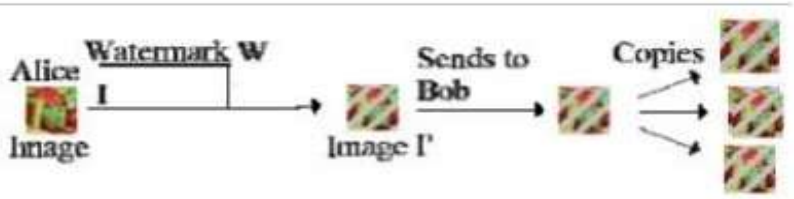


Fig. 5[29] : Digital Watermarking

Significance of Digital Watermarking, for example, suppose, as seen above in Fig., Alice makes a unique picture and watermarks it before passing it to Bob. On the off chance that Bob guarantees the picture and offers duplicates to other individuals, Alice can remove her watermark from the picture, demonstrating her copyright to it. The proviso here is that Alice might have the capacity to demonstrate her copyright of the picture if Bob has not figured out how to change the picture such that the watermark is sufficiently harmed to be imperceptible, or included his own watermark such that it is difficult to find which watermark was inserted first.

Watermarking Classification:[30]

- Visible & Invisible Watermarking
- Robust & Fragile Watermarking
- Asymmetric & Symmetric Watermarking
- Public & Private Watermarking
- Steganographic & Non-steganographic Watermarking

Visible Watermarking

[27] *Id.* 22 at Pg. 297
[28] *Supr*a Note 17
[29] *Ibid.*
[30] *Supra* Note 24

Visible watermark is a translucent overlaid into a picture and is obvious to the viewer. Visible watermarking is utilized to show ownership and for copyright assurance.

Original Image **WatermarkedImage**

Fig.6[31]: Visible Water-marking

Water marking Techniques

Fig. 7[32]: Water marking Techniques

Digital Watermarking Life Cycle Phases:

A watermarking system is usually divided into three distinct steps:

- Embedding
- Attack
- Detection

[31] S*upra* note 17 at 340.

[32] Anthony T.S Ho, Jun Shen Hie Tan, "A Robust Digital Image-in-Image Watermarking Algorithm Using the Fast Hadamard Transform", Proceedings of SPIE Vol. 4793 (2003).

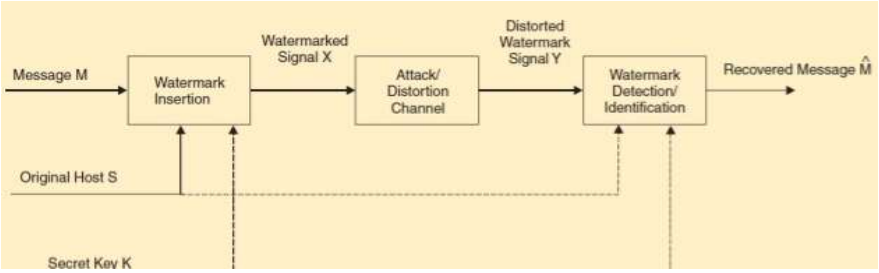


Fig.8[33]: Digital Watermarking Life Cycle Phases

Embedding

In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

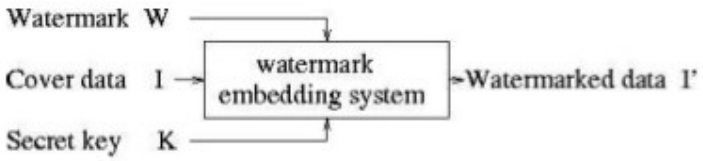


Diagram 9[34]: Embedding

Inputs to the scheme are the watermark, the cover data and an optical public or secret key. The output are watermarked data. The key is used to enforce security.

Extraction/ Detection

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted.

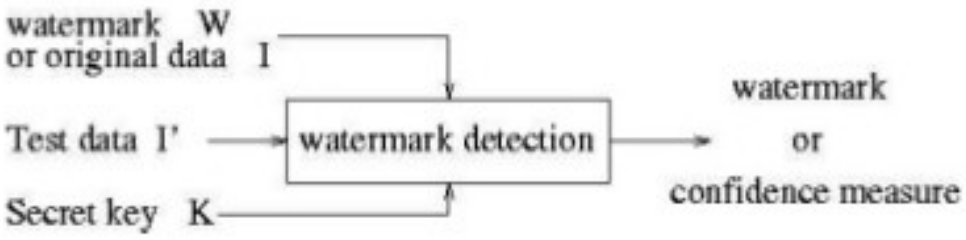
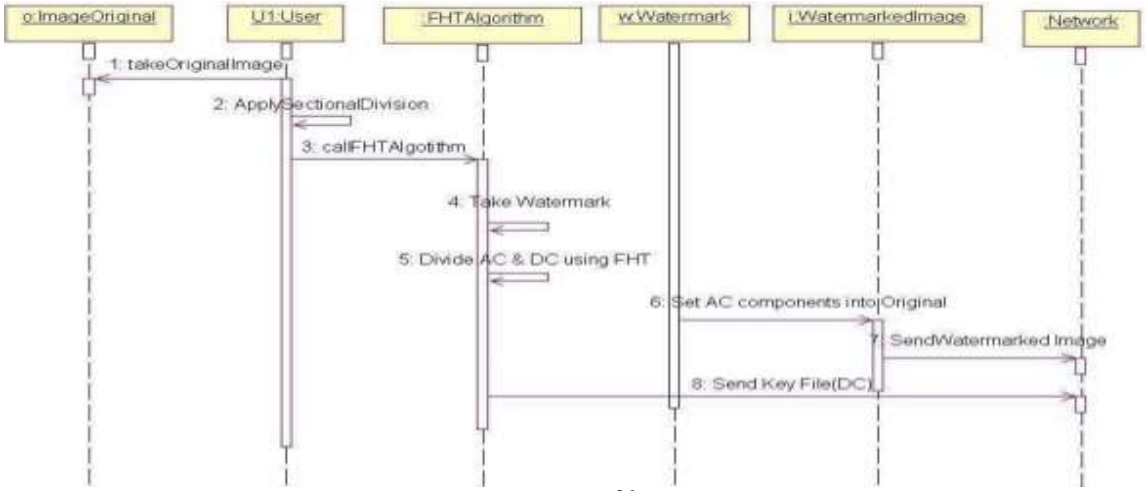


Diagram 10[35] : Extraction/ Detection

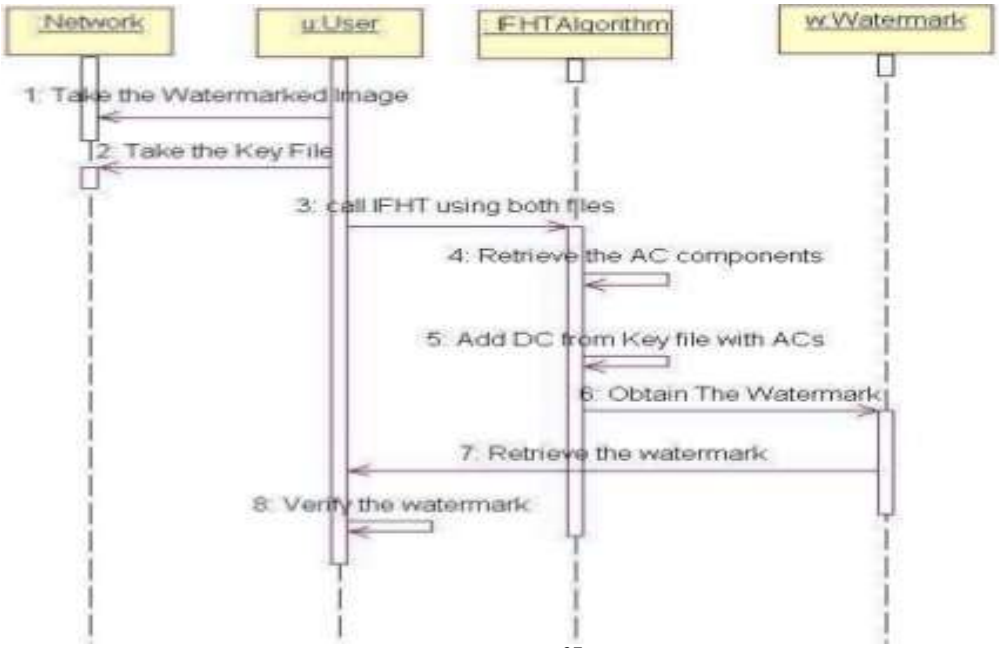
Inputs to the scheme are the watermarked data, the secret or public key and, depending on the method, the original data and/or the original watermark. The output is the recovered

[33] *Ibid.*
[34] *Ibid.*
[35] *Ibid.*

watermarked W or some kind of confidence measure indicating how likely it is for the given watermark at the input to be present in the data under inspection.

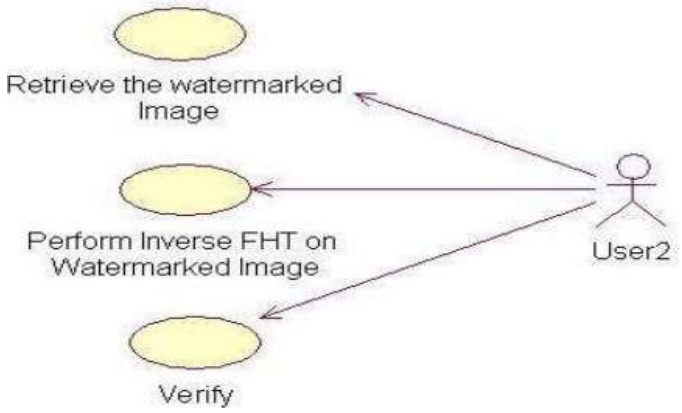


Sequence Diagram 11[36]: (Insertion)

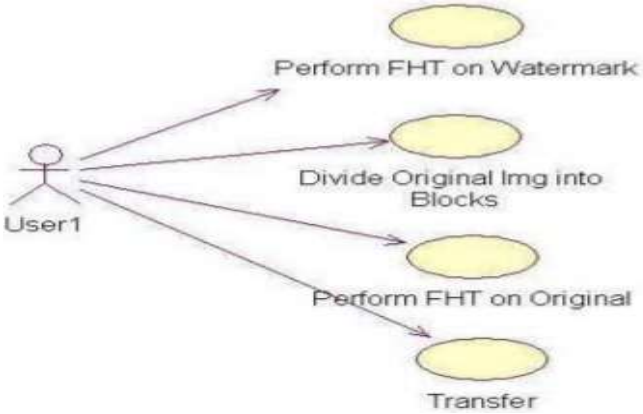


Sequence Diagram 12[37]: (Extraction)

[36] *Id*
[37] *Id*



Use Case Diagram13[38]: (Insertion)



Use Case Diagram 14[39] :(Extraction)

Watermarking In FHT Domain

The Hadamard matrix of the order *n* is generated in terms of Hadamard matrix of order *n-1* using Kronecker product, as:

$$H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}$$

Fast Hadamard Transform (FHT)[40]

Considering 8*8 sub-blocks of the whole image, the third order Hadamard transform matrix *H3* becomes:

[38] *Supra* note 16 at Pg. (342-34).
[39] *Ibid*
[40] *Supra* note 19 at Pg. 476

$$H_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

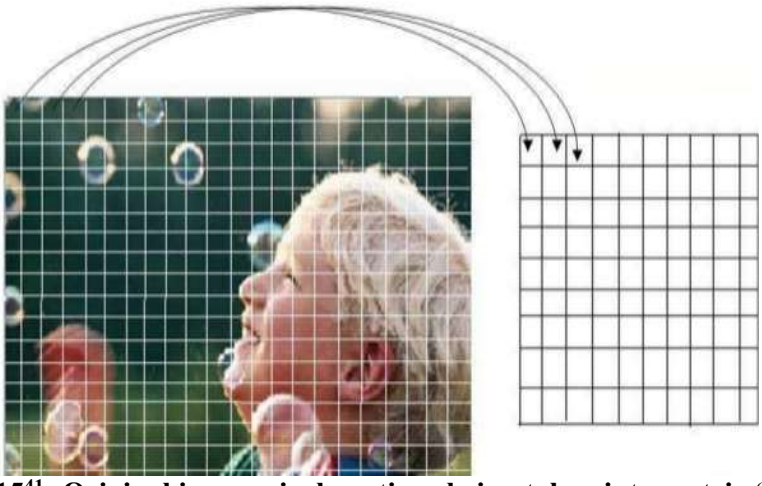


Fig.15[41]: Original image pixel portions being taken into matrix "U"

***The process of Insertion*:[42]**

- Transform watermark into FHT coefficients
- Randomly select sub blocks of Original Image to insert Apply
- FHT on each sub block
- Watermarked Image + Key File

[41] *Ibid*.
[42] *Supra* note 22.

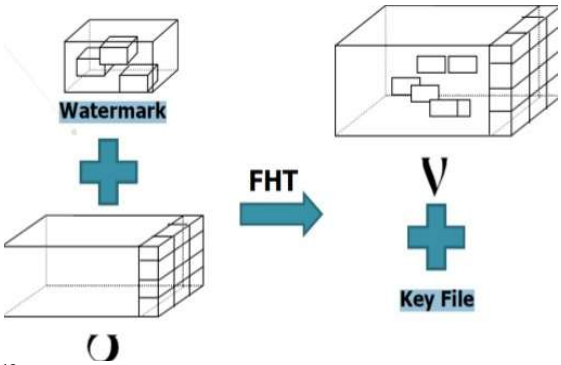


Fig.10[43] : Processing the Original Image....

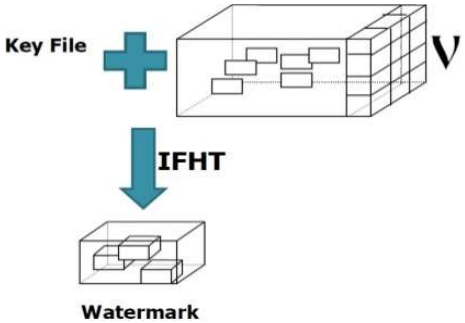


Fig.11[44] : Processing the Original Image:**Inverse Fast Hadamard Transformation: [45]**

$$[U] = H_n^{-1}[V]H_n^{*} = \frac{H_n[V]H_n}{N}$$

V : Transformed image
U : Actual image
Hn : N*H Hadamard matrix
H_n^{-1} : Inverse Hadamard matrix

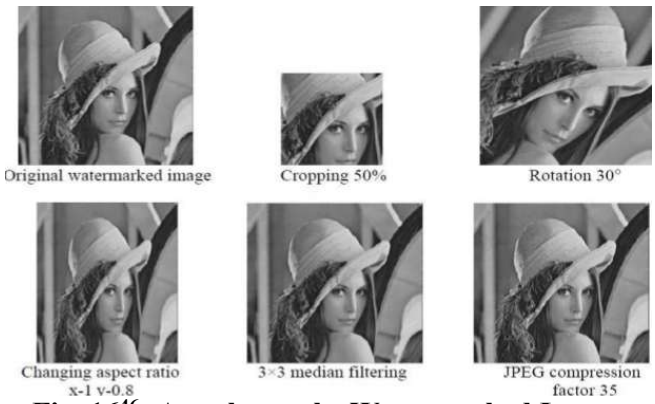


Fig. 16[46]: Attacks on the Watermarked Image

[43] *Ibid.*
[44] *Ibid.*
[45] *Supra* note 16 at 345.
[46] *Supra* note 30.

Experiment Result:[47]

Image operations	Extracted watermark	Correlation
Sharpening 3×3		0.9573
1 rows 1 column removed		0.9866
Frequency Mode Laplacian removal		0.9580
Scaling 0.75		0.9354
JPEG Compression of factor 30		0.8688
Change aspect ratio x_1.00_y_1.20		0.8199

The experimental results show that the proposed method is robust against approximately 70% of attacks. For sure when compared with previous, it is found to be more robust against various attacks. It also refers significant advantage in terms of shorter processing time and the ease of hardware implementation than many common transform techniques. Digital watermarking has risen as a fundamental security technology, completely corresponding to encryption-based secure transmission and copy protection. This technology is generally appropriate to all electronic data administrations and frameworks where information insurance, security, and intellectual property rights are required. Notwithstanding, viable uses in fields, for example, digital cam, DVD, advanced TV, electronic commerce, and law implementation have not been explored.[48] Basically the importance of Digital Watermarking are: *Copyright Information, On-line music industry and News gathering using digital cameras.*[49]

C. Biometric Approach – Cyber Space

A Biometric Approach as 'Another Approach' whereby the security undertakings of individual verification and key administration against encroachments in copyright are being ensured. From the Greek importance life (bio) and metric (to gauge), the expression "biometrics" alludes to those advances which is utilized for measuring and examining a man's physiological or behavioural attributes. Despite the fact that in all actuality, biometrics additionally alludes to ensuring system and physical security through the measures of physical and behavioural biometric systems.[50] Biometrics is measurable attributes particular to a single person. Face identification has differing applications particularly as an ID arrangement which can meet the crying needs in security zones. While customarily 2D pictures of countenances have been utilized, 3D sweeps that contain both 3D information and enrolled shading are getting to be simpler to secure. Prior to 3D face pictures can be utilized to recognize an individual, they oblige some manifestation of starting arrangement data, regularly in light of

[47] *Ibid.*
[48] *Id.* at 298.
[49] *Supra* note 7.
[50] Kenneth Kiesel, "*Biometrics: Beyond The Gummy Finger*", GIAC Security Essentials Certification (GSEC), Practical Version 1.4b, July 30, 2004.

facial peculiarity areas. It takes after this by a dialog of the calculations execution when obliged to frontal pictures and an investigation of its execution on a more perplexing dataset with noteworthy head posture variety utilizing 3D face information for identification gives a guaranteeing course to enhanced execution. Another is- ***Spoofing,*** which is a method, hackers utilize to gain access to unauthorized data or a system by posing as an authorized host or user. Biometric spoofing is performed by capturing an individual's biometric characteristic used for authentication and once obtained, utilizing it to claim the identity of such individual. Most notably, Matsumoto and colleagues, from Yokohama National University in Japan, developed a method to spoof fingerprint devices making a mold from plastic, originating from both a live finger and a latent fingerprint. Artificial fingers were then created from the casts using gelatine, commonly used for confectionary, where the resultant casts were termed "gummy fingers" [51]. Secondly , Lisa Thalheim and Jan Krissler for magazine while in a less rigorous fashion, demonstrated the vulnerability of a variety of biometric technologies through simple techniques for fingerprint spoofing such as: (1) by breathing on the fingerprint scanner to reactivate the latent fingerprint, (2) by using a bag of water on top of the latent fingerprint, (3) by dusting the latent fingerprint using graphite powder, stretching adhesive film over it and applying pressure, and [52](4) by using wax casts and silicon moulds. Most recently, Marie Sanstom conducted similar experiments this year (2004) for her Master's thesis, dispelling vendor's claims of anti -spoofing enhancements of optical and capacitive scanners. Nine different systems were tested at the CeBIT trade show in Germany and all were deceived[53]. Moreover, when it comes to ***Anti-Spoofing[54],*** in this system, security is based upon the founding principles of availability, integrity, and confidentiality. Anti-spoofing techniques are designed to enhance confidentiality by deterring hackers from gaining unauthorized access. An important aspect of anti-spoofing is to ensure that increased security does not occur at the cost of availability. Implementation must not come at a cost that makes availability (access to data) untimely.

Existing anti-spoofing techniques for fingerprint devices use:

- Medical-type measurements –pulse
- Change based measurements–temperature, perspiration; or
- Single skin attributes –colour, skin thickness, conductivity.

Systems can be designed and implemented to operate under one of the following three methods, like - query/response (randomization), after all fingers are enrolled, application randomly selects finger(s) required to present for authentication; combination –multiple fingers are enrolled in a user defined sequence this same sequential presentation is then required for authentication; complete - all fingers enrolled are required for authentication. Therefore, there are other methods too for determining anti-circumvent attacks, namely: *Liveness detection*, i.e. determining whether an introduced biometric is coming from a live source or not, has been suggested as a means to circumvent attacks that use spoof fingers. The goal of liveness testing

---

[51] Harris Tom, "How Finger Print Scanners Work" (June 22, 2004), *available at*: http://travel.howstuffworks.com/fingerprint-scanner.htm/printable (last visited on May 17, 2025.

[52] Schuckers SAC, "Spoofing and Anti-Spoofing Measures" 7(4) *Information Security Technical Report* 56–62 (2002). Stephanie A. C. Schuckers, Ph.D., Spoofing and Anti-Spoofing Measures, Clarkson University and West Virginia University, Article for Elsevier Information Security Report on Biometrics, Dec. 10, 2002, *available at*: http://www.citer.wvu.edu/members/publications/files/15-SSchuckersElsevior02.pdf (last visited on 17 Nov. 17, 2024).

[53] Marie Sandstrom, "Liveness Detection in Finger print Recognition Systems" (June 04, 2004), *available at*: http://www.ep.liu.se/exjobb/isy/2004/3557 (last visited on May 17, 2025).

[54] *Ibid.*

is to determine if the biometric being captured is an actual measurement from the authorized, live person who is present at the time of capture. Ideally, systems should measure for liveness simultaneously with the capture and authentication of the biometric data.

Another is *Perspiration*[55]**,** although not used in traditional minutia or pattern recognition systems, sweat glands and pores reside in the human fingertip that produce perspiration. Skin pores, like fingerprints, never spontaneously change or disappear but remain in their relative constant positions moistening the fingers with sweat. *Doctor Stephanie A. C. Schuckers and a small group from the Biomedical Signal Analysis Laboratory (BioSAL) have developed a method for liveness detection with fingerprint scanners.* They have developed an algorithm for the detection of a perspiration pattern over the fingertip skin. This algorithm quantifies the sweating pattern and makes a final decision about the liveness of the fingerprint presented. Due to the high dielectric constant of sweat, capacitive scanners are well suited for fingerprint authentication systems with perspiration detection. The sweat on the skin surface increases the capacitance between the finger and scanner resulting in an enhanced darker image capture. The key to this technology is based upon the physiological fact that perspiration starts from the pores and transverses along the ridges into the valleys. This perspiration creates time sensitive images that display the darkening ridges as the area is moistened with sweat. The capture of this process produces core perspiration information and patterns. The designed algorithm utilizes both static, perspiration beginning at the pores, and dynamic, image darkness transition over a five second period, approaches to authenticate and liveness validation. Two images are captured within this five second period and provide the data required for the algorithm to determine the perspiration pattern. System anti-spoofing is based upon the difficulty in recreating the perspiration pattern resulting from the static approach. This algorithm prevents an attacker from simply presenting an artificial or cadaver finger moistened with a solution equivalent to sweat and being authenticated. The BioSAL group is aggressively analysing their algorithm, striving to reduce the current five-second acquisition time. Next is, *Ultra-sound*[56], ultra-sound technology has been incorporated into a number of diagnostic systems utilized in the medical profession. Optel claims to have enhanced this technology in an Ultrasonic fingerprint scanner that is “impossibile” to fake. Optel’s claims are based upon the fundamentals that acoustic waves are mechanical in nature and their properties are affected by the mechanical properties of materials. Any acoustic waves received that are inconsistent with those of live tissue are discarded. Optel's new approach can additionally check for pulse as a second indication of liveness. This is accomplished by measuring changes in time caused by blood flow during the scan.

Then comes, the *Spectroscopy*[57], which is the science that describes how light is affected by a substance with which it interacts. Light comprises different wavelengths (colors) each producing unique characteristics of a substance. Skin is comprised of many different layers. When broadband light is used to illuminate the skin, a portion of the light is diffusely reflected and shows the effect of a number of physiological characteristics of the skin and underlying tissue that it passed through including[58]. The chemical and structural composition of skin tissue and its optical response produce a unique spectrum. Of greater importance to security, specifically anti-spoofing, is the premise that the compositional effect is extremely

[55] *Ibid.*
[56] *Supra* note 48.
[57] *Ibid.*
[58] Lumidigm Inc., “The Science Behind Lumi Guard”, *available at*: http://www.lumidigm.com/PDFs/The Science Behind LumiGuard -4.pdf (last visited on May 20, 2025).

characteristic of "living" human tissue. Lumidigm Incorporated has developed a deep tissue biometric technology (Lumi Guard) based on spectroscopy of visible and infrared light and the unique characteristics of human skin tissue. Next is, *Blood Vessel, a* Bionics Corporation designed an authentication system based upon the recognition of blood vessel-patterns within the fingertip. As with all biometric technologies the postulation is that no two vessel-patterns are the same. This uniqueness is claimed to hold true even for identical twins. The technology is similar to an optical fingerprint scanner using infrared light to permeate into the finger and a high quality CCD camera to capture the blood vessel pattern. Unlike fingerprints, the vessel pattern does not generate any latent images that can be utilized for spoofing. Research has shown that the epidermal tissue beneath the fingernail forms in a very unique parallel structure. During normal growth, the fingernail travels over the nail bed in a tongue-and-groove fashion. *On the off chance that a biometric recognizable proof framework had been set up before September 11, the disaster may have been kept away from as a few of the terrorists included were at that point on government watch arrangements of suspected terrorists.*[59] The need to have the capacity to robotize the distinguishing proof of people will get to be progressively imperative in the advancing years; watch records are expanding in size and it is no more reasonable to anticipate that human migration specialists will have the capacity to stay up with the latest with the substantial number of individuals on these rundowns. Biometric frameworks can work in check or ID modes relying upon their planned utilization. As a rule, there are three ways to validation.

In place of slightest secure and minimum advantageous to most secure and most helpful, they are:

- Something you have - card, token, key.
- Something you know- PIN, password.
- Something you are - a biometric.[60]

The human face plays an irreplaceable role in biometrics technology due to some of its unique characteristics. The first task needed after the capture of an image is an initial alignment. The features commonly used to identify the orientation and location of the face is the eyes, nose, and mouth. This approach is the standard used on most facial biometric algorithms. After this stage, processing varies based on whether the application is identification or verification. Identification is the process of determining who someone is. Verification only needs to confirm that a subject is the person they claim to be[61]. In identification, the system compares the captured image (probe) to the gallery. The type of comparisons made depends both on the biometric used and on the matching algorithm in question. After the comparison, the system returns a rank ordering of identities. The face verification compares features from the captured image (probe) to those belonging to the subject of the identity claim. After the comparison, the system returns a confidence score for verification. If this score is above a certain threshold, the system verifies the individuals identity. This bar code is unique to each individual and becomes the identifier for authorization system. The nailbed is protected and hidden by the fingernail significantly decreasing the capture and utilization of this biometric as a spoofing mechanism. AIMS claims, it is virtually impossible to obtain a false-positive match, i.e., the finger must

[59] I.J. Image, "Graphics and Signal Processing" 8 *MECS* 43-49 (Aug. 2012), *available at*: http://www.mecs-press.org/ (last visited on May 20, 2025).
[60] A.K. Jian, R. Bolle, *et.al.* (eds.), *Biometrics personal identification in networked society* (Kluwer, Norwell, MA, 1999).
[61] R. Osadchy, M. Miller, *et.al.*, "Synergistic face detection and pose estimation with energy-based model", in *Advances in Neural Information Processing Systems* 1017-1024 (MIT Press, Cambridge, 2005).

be a living organism[62]. Different vendors use: *The physical biometric strategies which incorporates all like*: fingerprinting, hand and finger geometry, facial recognition, iris and retinal checking, and vascular example recognition. Specifically, research concentrated on enhancements of liveliness testing to traditional authentication and innovative technological advances of finger authentication beyond use of fingerprints. So, they can say that this biometric identification and verification proof includes for deciding, 'who a man is' and biometric check is figuring out whether a man is who they say they section of land. The educator , Eric Cole, left this for everlasting proclamation engraved into our memory : *"What can be utilized for Good, can likewise be utilized for Evil "*. This nonstop clash is ever display in our universe of digital security. The utilization of fingerprints and consolidation of unique finger impression scanners into validation frameworks was intended to fortify the security of data frameworks. Capacity to catch, reproduce, and farce unique mark scanners transitioned this security improvement into a powerlessness. It is imperative that System integrators and Security professionals maintain visibility with emerging technologies and keep abreast of security vulnerabilities.

IV. CONCLUSION AND SUGGESTIONS

> *"We must take care to guard against two extremes equally prejudicial; the one, that men of ability, who have employed their time for the service of the community, may not be deprived of their just merits, and the reward of their ingenuity and labour; the other, that the world may not be deprived of improvements, nor the progress of the arts be rewarded"*[63]

In this fast pacing world when internet or the World Wide Web has become a way of life and it has become as easy as the click of a button to share distribute, disseminate, information or content it is becoming increasingly difficult to protect those very rights or content. In our opinion one of the shortcomings of the protection provided by DRM is that:

a. it provides right holder oriented protection only where the consumer is at the most neglected. TPMs being the first method employed for the protection of digital content of right holders provide minimum protection than needed. It is a method in which it is right holder who has control over use of his work and determining the extent to which one can access said work. TPM provides mechanism called metadata for the storage of the authorised content by a consumer allowed by right holder. The right holder through this method may protect his work by fencing various technologies such as encryption, authentication, access control, digital watermarking, temper-resistant, hardware and software and risk management architectures.
b. as TPM holds small sphere for providing protection is turned out to be a failure as with rapid developments, software and programs are being developed to decode the said protection immediately as soon as it is adopted. The protection provided by TPM measures seems to be incomplete without the next measure employed in DRM i.e. Anti-Circumvention that supplements the former in providing protection to the right holders.

[62] AIMS Technology Inc., "AIMS Biometric Technology", *available at*: http://www.nail-id.com/faqs.html (last visited on May 25, 2025).
[63] *Sayre* v. *Moore* (1785), cited in *Cary* v. *Longman* (1801), 1 East 358, 362 n.(b), 102 E.R.138,140n.(b).

c. when taken into observation it is reflected that the anti-circumvention regulations in addition to punishing acts that circumvent, also make illegal any such activities that may be used for such circumvention and also their dissemination or distribution thus it extends to the punishing of preparatory activities, which seems to be a new step towards such security. Unlike TPM the protection provided by anti-circumvention regulations seems to be more effective as it provides a statutory backup as well and not just the technological means.

Suggestions

a. the international conventions WCT which provide for protection of copyright deal with provisions for anti-circumvention regulations, under Article 11 – 12. This conventions obligate the member nations to enact and implement legal protection to the right holders against circumventions which is prohibited and violative of the rights of the authors or right holders. USA was amongst the first nations to incorporate the concept of anti-circumvention regulations.
b. Section 1201 of the Digital Millennium Copyright Act 1998, herein after referred to as DMCA, provides for such measures. DMCA in its operation distinguishes and specifically applies anti-circumvention regulations to both access control and usage control in terms of technological protections measures. The security provided is almost similar in both cases with one difference that in case of usage control only preparatory activities are considered infringing while in case of access control both preparatory activities as well as the actual act of circumvention are scrutinised as infringing.

This would be a good time to mention that India is not a member of WCT and WPPT and thus does not have any specific provisions dealing with anti-circumvention regulations. It is noteworthy that India is progressing to enact such regulations and the Copyright (Amendment) Bill, 2025 draft rules which proposes a bigger shift towards digital-first royalty management, but are still awaiting finalisation after stakeholder consultation which is pending seeks the implementation of them.