International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 8 Issue 07 Series. I || July 2019 || PP 01-07

A Focused Study on Various Techniques of Digital Watermarking

Diksha Kumari [1], Vishal Shrivastava[2]

Department of Computer Science and Engineering Arya College of Engineering and I.T., Jaipur
Corresponding Author: Diksha Kumari

Abstract-*Advanced substance can as often many times duplicated by unapproved individual and guarantee to his possession. Be that as it may, we don't have the foggiest idea who the real proprietor of that substance is. Advanced Watermarking is a significant issue to take care of this sort of issue. Since the advanced information is moved over the web which may damage the computerized information like altering of information and so on. Subsequently the requirement of computerized information's security has been expanded with the headway in the innovation. Watermarking is a strategy used to ensure the advanced information. Computerized watermarking is a procedure by utilizing which client can have the copyright of its item which keeps the information from altering. Numerous systems are accessible for video watermarking like Discrete Wavelet Transform, Least Significant Bit Technique and so forth. [1].The characteristics of watermarking are for duplicate control, For fingerprinting, For ID of proprietorship, For Authentication, Monitoring of advanced video communicate, In video labelling and so on [2]. During this paper the different major parts of the advanced watermarking alongside essential model, properties and different work accomplished for the improvement of the procedures considered for digital watermarking are mentioned.*

Index Terms— *Digital watermarking, Images, DCT, Embedding, Cryptography, Hidden.*

Date of Submission: 25-06-2019 Date of acceptance: 10-07-2019

I. INTRODUCTION

Because of upgrade of data innovation appropriation of computerized information is turned out to be simple. Expanding being developed, builds security strings of information. It is significant issue to shield sight and sound information from numerous assaults, for example, forging, theft and malevolent maniple. To give answer for some assaults number of instrument utilized, advanced watermarking is one of them. Watermark-It is a name, a tag, a data holder which addition into sight and sound information to make unique information secure from unlawful control and appropriation.

The way toward inserting the watermark into a computerized information is known as Digital Watermarking. Watermarking is the way toward inserting information called a watermark into a sight and sound item, for example, pictures, video, or content for their copyright protection[3]. The installed watermark might be either obvious or undetectable. The idea of computerized watermarking is related with the steganography.

Characterisation of it is done as secured composing, that conceals the significant message in a secured media while, computerized watermarking is a method for concealing a mystery or individual message to give copyrights and the honest information. The inserted watermarks are hard to evacuate and regularly intangible, could be as content, picture, sound, or video. The implantation of mystery watermark in advanced information, regardless of how much imperceptibleit might be. Anyway it prompts some corruption in the resultant inserted information. To conquer this constraint and to recover the first information, reversible watermarking has been executed which is considered as a best methodology over the cryptography.

The advanced watermarking framework basically comprises of a watermark Embedder and a watermark indicator. While utilizing watermark Embedder watermark is embeds onto the spread sign and utilizing watermark locator identifies the nearness of watermark signal. A substance called watermark key is utilized during the way toward installing and recognizing watermarks.

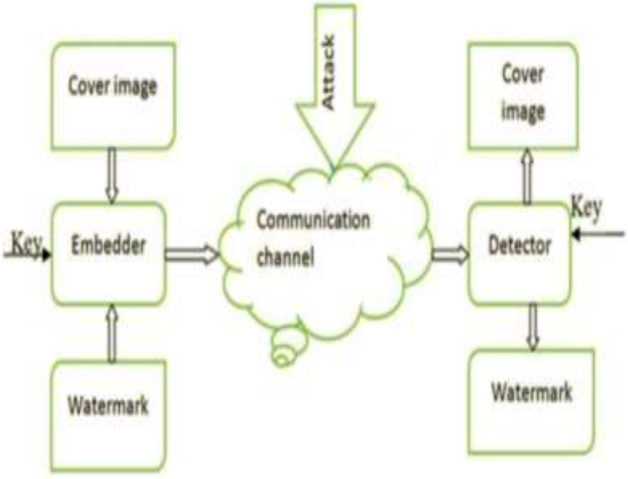

Fig. 1 General model of Digital Image watermarking.

II. VARIOUS KIND OF DIGITAL WATERMARKING

Two kinds of watermarking procedures are as pursues: Visible watermarking Invisible watermarking

A. Visible Watermarking

During the implementation of this system the implanted watermark is noticeable to the end point client. It is previously available strategy of watermarking. The watermark is inserted on the spread page of the picture. It is the primary technique for watermarking endeavoured with the goal of security. It is inserted so that it is unmistakably obvious by the unaided eyes to the client. In this watermark is included the spread picture. Along these lines watermark is unmistakable to the end point client plainly.

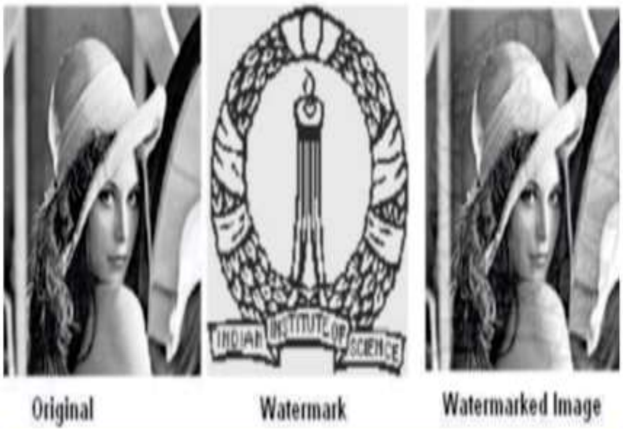

Fig. 2 Visible Watermark.

B. Invisible Watermarking

Watermarking system termed as invisible watermarking is that sort of system which implanted watermark isn't unmistakable to the watcher. In this the additional watermark on the computerized information can't be easilyviewed. The watermark is inserted on the overlaid picture. This watermark isn't noticeable to the end client yet at the same time it very well may be distinguished by utilizing calculations or different procedures. In this watermark is carefully installed in the picture. These sorts of watermarks are utilized to evidence the proprietorship. Additionally, this is used to recognize the mishandling of the item. Likewise, it is considered as the reinforcement for visible watermarking [4].

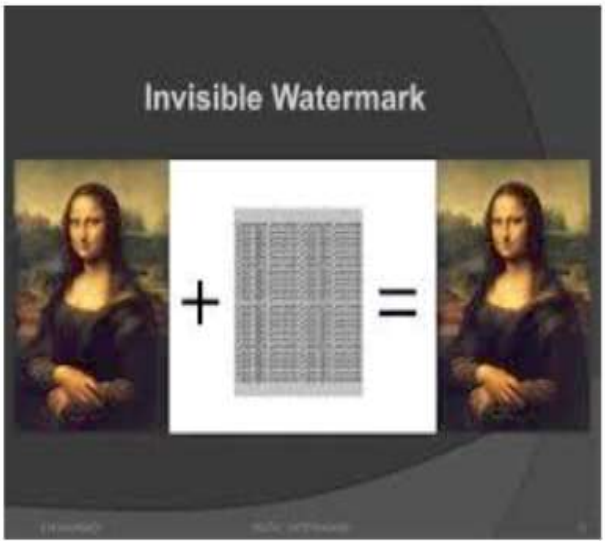

Fig. 3 Invisible watermarking.

And furthermore, on the premise a few other criteria's computerized watermarking can be additionally characterized of subsequent sorts:

Table I. Types of watermarking basis of different Criteria.

S.No.	Criteria	Classification
1.	Watermarking Type	1. Noise: pseudo noise, Gaussian random and chaotic sequences 2. Image: Any logo, Stamp Image etc.
2.	Robustness	1. Fragile: Easily Manipulated. 2. Semi-Fragile: Resist from some type of Attacks 3. Robust: not affected from attack
3.	Domain	1. Spatial: LSB, Spread Spectrum 2. Frequency: DWT, DCT, DFT, SVD
4.	Perceptivity	1. Visible Watermarking: Channel logo 2. Invisible Watermarking: likeSteganography
5.	Host Data	1. Image Watermarking 2. Text Watermarking 3. Audio Watermarking 4. Video Watermarking
6.	Data Extraction	1. Blind 2. Semi-Blind 3. Non- Blind

III. CHARACTERISTICS OF DIGITAL WATERMARKING

This segment portrays the properties of advanced watermarking calculation:

- **Imperceptibility:**Essential necessity of advanced watermarking is to have the watermarked picture should resemble the other alike as the initial picture. This affirms there isn't much corruption on the initial picture. The installed watermark ought not to be obvious to human eye. To compute the subtlety, by and large Peak Signal to Noise Ratio (PSNR) is utilized.
- **Security:**The watermarking framework ought to be verified for example programmer ought not to be in position to remove the watermark without having the learning of implanting calculation. Watermarking framework must be fit for remain against various assaults. Assaults attempt to evacuate, alter or implant into the watermark. Assaults are fundamentally ordered in two distinct sorts for example latent assault and dynamic assault. Uninvolved assault just identifies the watermark data, while dynamic assault attempts to alter the watermark data.
- **Robustness:**The ability of endurance of watermark adjacent to both authentic and ill-conceived assaults is eluded as strength. Robustness relies upon watermarks data limit, deceivability and quality. For the most part a decent watermarking calculation ought to be vigorous against channel preparing, noise expansion, geometrical changes, for example, revolution, scaling, interpretation and loss pressure, for example, JPEG pressure.
- **Capacity:**Capacity of the watermarking framework portrays inserting of most extreme measure of watermark data in single information. The higher limit of implanting data in information can be gotten by bargaining either intangibility or power of calculation.

- **Complexity:**The time and exertion expected to insert and recovered the watermark data is called as multifaceted nature of the watermarking framework. The mind boggling calculation in watermarking framework needed more programming and equipment assets to execute it that brings about expanding the calculation cost. To diminish the computational expense of watermarking framework, it should be less perplexing. Information less perplexing watermarking calculations is executed.
- **Invertibility:**This characteristic of advanced watermarking framework portrays the likelihood of creating unique information during the extraction procedure for watermarking [5].

IV. WATERMARKING TECHNIQUES

During this segment different slanting watermarking methods have been examined.

1. **DWT Transform:**During the following strategy of watermarking picture is subdivided into four sections. These are as horizontal part, corner to corner part, vertical part, and estimation part. The picture is isolated into four sections for changing over the picture into lower resolution goals picture. The procedure is rehashed for figuring the numerous scale wavelets decaying. DWT is progressively ideal procedure for watermarking in light of the fact that it performs calculations in all respects precisely. The positive purpose of this system is that it is powerful to deal with the commotion in the picture.
2. **DCT Transform:**It represents Discrete Cosine Transform. The fundamental component of utilizing this procedure is that it gives the great sign estimation by utilizing certain coefficient esteems. With the help of this strategy utilising numerous calculations for installing the watermarking on picture takes place. The principle bit of leeway of this method is that it is very quick as contrast with different strategies. During implementation of this strategy the watermark is implanted on the inside recurrence groups on account of deterioration of the picture. This system is progressively hearty to lossy compressions as contrast with others.
3. **DFT Transform:**Discrete Fourier Transform dependent watermarking strategy, the brilliance of the edge that is watermarked is gotten and the coefficient's magnitude is engaged to process DFT. In this system backwards DFT is additionally connected. This procedure is powerful and impervious to different assaults like pixel evacuation and pivot.

V. DIFFERENT WORKS DONE IN THE FIELD

During this research by Monika Patel [6] et al. main focus was on portrayal that the advanced information is anything but difficult to alter and modify when tit is transmitted over the web. To determine this issue the idea of watermarking is created. In watermarking the data identified with the copyright or validation is implanted on the first information which keeps the information from unapproved get to. Different algorithmic calculations can be utilized for installing the watermark on the information. The choice of calculation relies on the idea of the information.

During this author Bhattacharjee, T [7] et al.. characterizes a technique used for information stowing away and sharing mutually. In this above all else picture is partitioned into little offers and afterward these offers are implanted into the spread picture to conceal the information. Inserting of the information is done in DCT area. It utilizes m-cluster spread range balance. This is a practically equivalent to strategy as (k, n) plot covertly sharing. Based upon the quantity of clients that are engaged with deciphering process, the quality access control can be gotten to or got after recreation it is demonstrated that the proposed procedure is hearty in nature and powerful to the info or yield of the framework.

As mentionedin this paper by Vinita Gupta [8] et al., it is characterized that Digital watermarking is a procedure to conceal the information behind any picture, sound, video and so forth. It is kind of cryptography. In this paper picture watermarking is clarified. Different strategies are likewise examined for picture watermarking. Utilizations of picture watermarking are additionally characterized. A few components and properties are additionally talked about alongside a review performed in New York based on picture watermarking.

During present scenario PreetiParashar [9] et al,put forward that generally information goes over the web with the end goal of correspondence. Therefore the security of computerized information is the fundamental concern. In this creator characterizes, that advanced watermarking is a strategy which is utilized to verify the secret information. It keeps the information from duplication or altering by concealing the mystery message in the first data or information. The areas arranged the strategy of picture watermarking as spatial space; change space and so forth spatial area is a system which chips away at the premise of pixels. Also, the space, recurrence area deals with the change coefficients o the picture. During the paper authormainly mentioned about the spatial and change area alongside their points of interest and hindrances.

The creation of a technique byMiroslavDobsicek [10] that has where the substance is encoded with one key and can be unscrambled with a few different keys, the relative entropy among scramble and one explicit decode key.

The built up of online verification framework by Yusuk Lim, ChangshengXu and David Dagan Feng, 2001 [11]. If there should arise an occurrence of watermark inserting framework, it is introduced in the server as application programming that any approved client, who approaches server, can create watermarked picture. The conveyance can utilize any sort of system transmission, for example, FTP, email and so forth. When picture is conveyed to remotely, customer can access to validation site page to obtain check of picture.

Another strategy which controls "flappable" pixels to implement explicit square based relationship so as to insert a lot of information without causing observable ancient rarities by Min Wu and Bede Liu, June 2003, proposed [12]. The shrouded information would then be able to be extricated without utilizing the first picture and can likewise be precisely separated after great printing and filtering with the assistance of a couple of enrolment marks.

During the year 2007, there was a proposal of information security by Nameer N. EL-Emam that utilize LSB inclusion steganographic technique. During the implementation of this methodology, high security layers have been proposed through three layers to make it hard to get through the encryption of the information and befuddle steganalysis too [13].

A clarification is provided by Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al-Taani, 2005, that a strategy with three fundamental advances. In the first place, the edge of the picture is recognized utilizing Sobel veil channels. Second, the least huge piece LSB of every pixel is utilized. At last, a dim level network is connected utilizing a fluffy methodology and the ASCII code is utilized for data covering up. The earlier piece of the LSB speaks to the edged picture after dim level network, and the staying six bits speak to the first picture with almost no distinction conversely. The given technique implants three pictures in a single picture and incorporates, as an exceptional instance of information installing, data stowing away, recognizing and validating content inserted inside the computerized pictures [14].

In year 2008, Prof S. K. Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, DebashisGanguly, Poulami Das has proposed a heuristic way to deal with conceal tremendous measure of information utilizing LSB steganography method. The resultant stego-picture was contortion less. Additionally, they have given much accentuation on space multifaceted nature of the information concealing method [15].

During the year 2008 a strategy chips away at more than one picture utilizing the idea of document hybridization presented by G. Sahoo and R. K. Tiwari. This specific strategy executes the cryptographic method to implant two data records utilizing steganography and because of this reason they have utilized a stego key for the installing procedure [16]. Actually, the implanting of high-entropy information (regularly because of encryption) changes the histogram of shading frequencies in an anticipated manner. Along these lines, so as to get greater security in our recommended technique, we have inserted a whole picture behind another picture of double the size of target picture for a surprising change in the last picture.

During the information implementation of this paper a strategy is proposed to ensure computerized personality reports against a Print Scan assault for a verified ID card confirmation framework by Peyman Rahmati, Andy Adler and Thomas Tran (2013) , ―Watermarking in E-business [17]. The current PS task forces a few bends, for example, geometric revolution and histogram mutilation on the watermark area which may cause the loss of data. The proposed framework evacuates contortion of the PS task: - sifting, restriction, binarizitation, pivot and editing. The proposed verification framework separates the watermarks inside the ID card's holder photograph, place in the decoder and afterward looks at it with the ID card individual number. On the off chance that the removed watermark and the ID card individual number are the equivalent, the character of the client/client will be confirmed generally personality will be deprived of.

During this paper, another method for sorting watermark procedure through picture displaying is examined by Neil F. Johnson,ZoranDuric and SushilJajodia. [18] The picture displaying called ‗alpha channel synthesis' utilizes steady veil. Two pictures with level cover and slow veil are utilized to make watermark that changes dim estimations of pixel in the picture. A technique for watermark recuperation by applying converse change to the contorted pictures is appeared. The picture is watermarked utilizing the variant of Digimarc'sPictureMark watermarking channel that is accessible with Adobe PhotoShop and the picture is contorted by applying the Stirmark instrument of relative change.

During this Paper, calculation for installing watermarking is displayed by utilizing DWT and encoded with QR codes by Vinita Gupta, AtulBarve(2014). [19].At this point spread picture is chosen and DWT is connected on it. A key K is chosen to produce the QR code as mystery key. QR code and watermark picture is scrambled by utilizing XOR task. At that point the scrambled watermark is inserted into the spread picture and backwards DWT is connected on the implanted watermark picture. In support of extraction, essentially apply the DWT on the spread picture. This calculation is very basic in view of the utilization of straightforward X-OR task for encryption. This calculation is appropriate on various sort of assaults on watermarked pictures like JPEG Compression, Possion Noise Attack, Salt and Pepper Noise and Gaussian Noise.

VI. SPECIFIC REQUIREMENTS OF WATERMARKING TECHNIQUE

By and large, advanced watermarking systems should fit in with some after necessities.

- **Invisibility:**the distinction among watermarked and unique interactive media must not be seen by unaided eyes, in particular, the nature of watermarked sight and sound have to be great.
- **Security:**everybody with the exception of legitimate one can't recognize watermark which is covered up in interactive media. Besides, watermarking calculation must be open, to be specific, the security of the watermarking framework ought not expand on assailants who don't have the foggiest idea how the framework functions.
- **Efficiency:**so as to be actualized effectively, the watermarking calculation must have great executing effectiveness, and it needn't bother with unique interactive media to separate watermark.
- **Robustness:**post the inserted media is prepared by computerized sign handling, (for example, separating, compacting, editing, honing, obscuring, and so forth.) the watermark still can be extricated at what time the nature of the interactive media is satisfactory.

VII. APPLICATIONS OF DIGITAL WATERMARKING

Expanding research on watermarking from the previous decades has been to a great extent propelled by its applications in copyright the executives and insurance.

- **Copyright Protection:**Digital watermarks can be utilized to distinguish and ensure copyright proprietorship. Advanced substance can be installed with watermarks delineating metadata recognizing the copyright proprietors.
- **Broadcast Observation:**It is the outstanding use of watermarking, which causes promoting organizations to follow the particular video communicated by a TV Channel or station. Inserting the watermarked video to the host video will give you simpler approach to track and screen to communicate.
- **Owner Recognition:**Additionally, it is the famous use of watermarking, that aide in recognizing the proprietor of video or picture. For example, copyright experts, where as opposed for giving copyright see each picture or video the watermark could be legitimately inserted in to the picture or video automatically.
- **Copy Management:**An additional understandable usage of watermarking is duplicate control which aides forestalling the unlawful duplicate of tunes or pictures of films and so forth. Where by installing watermark in melodies or pictures of motion picture would teach a watermarking good DVD or CD essayist to not compose the tune or film as it is an unlawful duplicate.
- **Transaction tracking:**By the help of assistance for watermarking Transaction Tracking can be accomplished by chronicle the exchange subtleties in the historical backdrop of a duplicate in computerized work. For instance issuing every beneficiary a lawful duplicate of motion picture by installing the watermark will help in following the wellspring of hole if there should be an occurrence of film spilled to the web.
- **Medical Field:**Medical picture watermarking is solitary of the significant utilizations of watermarking. Medicinal picture verification frameworks can verify therapeutic pictures as well as have the option to furtively convey helper data can be accomplished by watermarking strategy. Just the approved individuals of the clinic would along these lines have the option to adjust the substance of restorative picture.

VIII. CONCLUSION

Numerous papers are looked into with respect to the watermarking and its strategies. Every procedure that is considered some of them is progression in customary systems and some are bases for new proposed strategies. Every method is effective and has numerous favourable circumstances however on opposite side there are a few hindrances too. There are numerous sorts of watermarking is accessible. Obvious watermarking is plainly unmistakable to the end client while undetectable watermarking isn't noticeable to the end clients. Undetectable watermarking must be uncovered by utilizing a few calculations or systems. The works considered in the overview have taken any a couple of considered significant prerequisites of the watermarking past which the instruments are to be chosen like they can convey the every single real necessity of the computerized watermarking. For the further thought the things can be considered for the satisfaction of the real necessities of the computerized watermarking like Invisibility, Security, Efficiency and Robustness.

REFERENCES

[1]. M. Jacob, S. Mitra, “Video Watermarking Techniques”, IJRTE, Vol 4, pp. 1-4,2015.

[2]. L. K. Saini, V. Shrivastava, “A Survey of Digital Watermarking Techniques and its Applications”, IJCST, Vol. 2, pp. 70-73,2014.

[3]. M. Thapa, S.K.Sood, “Digital watermarking is used to hide the information inside a signal”.

[4]. S. Dhiman, O. Singh, “Analysis of Visible and Invisible Image Watermarking – A Review”, International Journal of Computer Applications, Vol. 147, No.3, pp. 36-38, August 2016.

[5]. S. Singla, R. Bansal, “Watermarking Methods for User Selection System As Visible and Invisible Using DWT”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 3, Issue 5, pp. 1743-1746, May 2014.

[6]. M.Patel,P.S.Sajja,” Analysis and Survey of Digital Watermarking Techniques”, ijarcsse, Vol 3, pp 203-210, 2013.

[7]. “Progressive quality access through secret sharing and data hiding scheme”Pp 5- 7,2014

[8]. V. Gupta , “A Review on Image Watermarking and Its Techniques”, IJMEIT ,Vol. 2, Issue 1, January 2014.

[9]. P.Parashar,"A Survey: Watermarking Techniques", 2014.

[10]. Dobsicek, M., "Extended steganographic system", 8th Intl. Student Conf. on Electrical Engineering, FEE CTU 2004, Poster 04.

[11]. Y. Lim, C. Xu and D. D. Feng, "Web based Image Authentication Using Invisible Fragile Watermark", Pan-Sydney Area Workshop on Visual Information Processing (VIP2001), Sydney, Australia, pp. 31 -34, 2001.

[12]. M. Wu and B Liu, "Data Hiding in Binary Image for Authentication and Annotation", IEEE Trans. Image Processing, vol. 6, Issue 4, pp. 528-538, Aug. 2004.

[13]. Nameer N. EL-Emam "Hiding a large amount of data with high security using steganography algorithm", Journal of Computer Science,pp. 223–232, April 2007.

[14]. Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al-Taani, "Data Embedding Based on Better Use of Bits in Image Pixels", International Journal of Signal Processing, Vol 2, No. 2, pp. 104-107, 2005.

[15]. S.K.Bandyopadhyay, D. Bhattacharyya, S. Mukherjee, D. G., PoulumiDas, "A Secure Scheme for Image Transformation", IEEE SNPD, pp. 490–493, August 2008.

[16]. G. Sahoo, R. K. Tiwari, "Designing an Embedded Algorithm for Data Hiding using Steganographic".

[17]. P. Rahmati, A. Adler, and T.Tran,"Watermarking in E-commerce", (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 4, No. 6, 2013.

[18]. Neil F. Johnson, ZoranDuric, and SushilJajodia. "A Role for Digital Watermarking in Electronic Commerce", http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.449.6184&rep=rep1&type=pdf.

[19]. V. Gupta, A.Barve, "Robust and Secured Image Watermarking using DWT and Encryption with QR Codes", International Journal of Computer Applications (0975 – 8887),Vol. 100, No.14, August 2014.

Diksha Kumari" A Focused Study on Various Techniques of Digital Watermarking" International Journal of Engineering Science Invention (IJESI), Vol. 08, No. 07, 2019, PP 01-07