A Review on Digital Image Watermarking and its Techniques

Sumi Choudhury\textsuperscript{1} Swati Agrawal\textsuperscript{2}
\textsuperscript{1,2}Department of Electronics & Telecommunication Engineering
\textsuperscript{1,2}Bhilai Institute of Technology, Durg (C.G.), India

Abstract— With the vast improvement in computer system and digital interactive media innovation, the need of ensuring the responsibility for media turns into a noteworthy issue. Watermarking is a procedure of concealing indistinct information into advanced media like content, audio, video and so forth. The significant parts of data covering up are security, indistinctness and strength. To expand security, a mystery key can be utilized to encode and decipher the watermark. In this paper, we show an audit on image watermarking and its procedures. There are a few systems that depend on spatial and change domain for watermarking. We additionally examine different properties and implementations of image watermarking. Past work in advanced watermarking is additionally assessed.

Key words: Watermarking, Key

I. INTRODUCTION

Nowadays, as computerized media are increasing more extensive fame, their security related issues are getting to be more noteworthy concern. Digital watermarking is a method which permits a person to include copyright sign or other check messages to digital data. Inside the field of watermarking, image watermarking especially has pulled in the attention of research scholar. A large portion of the research work is devoted to image watermarking when contrasted with sound and video. There might be 3 purposes behind it. Firstly, because of prepared accessibility of the test images, besides on the grounds that it conveys enough excess data to give a chance to insert watermarks effectively, and ultimately, it might be expected that any fruitful image watermarking calculation might be updated for the video too.

The goal is not to shield the substance from being replicated or stolen, however is to give a technique to validate the image and guarantee the respectability of the image. The best approach to understand this element is to implant a layer of the confirmation signature into the advanced image utilizing a computerized watermark. On account of the image being altered, it can undoubtedly be distinguished as the pixel estimations of the implanted information would change and don't coordinate with the first pixel values. There are numerous spatial and recurrence area procedures accessible for verification of watermarking. Watermarking procedures are judged on the premise of their execution on a little arrangement of properties.

These properties incorporate vigor, straight forwardness, watermarking limit, daze location and security. Watermarking plans are created by prerequisites of the application and all applications don't require each of these properties completely i.e. watermarking prerequisites are application reliant and some most alluring properties for these applications are clashing in nature. A gigantic exchange off among them is regularly included. Computerized mark is likewise a validation plan that is utilized for checking the trustworthiness and realness of the image content. There is need of a framework to stow away (for the most part encoded) information into other information. The “mystery” of the installed information is vital here.

Images can be represented in two ways in spatial domain and in transformation domain. Image in spatial domain is represented by pixel values and in transform domain it constitutes frequencies. In basic terms, change space implies the images is fragmented into numerous recurrence groups. To exchange a picture to its frequency representation, we can utilize a few reversible changes like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT). Each of these changes has its own particular qualities and speaks to the images in various ways.

Watermarks can be insert inside images by changing these qualities, i.e. the change area coefficients. If there should arise an occurrence of spatial domain, basic watermarks could be inserted in the images by changing the pixel values or the Least Significant Bit (LSB) values. Nonetheless more powerful watermark can be inserted in transform domain of images by refitting transform domain images.

II. ANATOMY OF DIGITAL IMAGE WATERMARKING

Advanced watermarking frameworks normally incorporate two essential segments: the encoder and the decoder. The information sources are the cover media information, the inserting security key, and watermarks in the watermark encoder. The encoder embeds a machine-coherent code (watermark) into sound, video, and pictures with variation implanting calculations, origination and plans by adjusting physical or electronic media and all watermarking methodology are controlled by private keys, which are allotted to the addition and extraction system to separate the watermark data appropriately and to warrant crucial security.

The yields are the security key and the watermarked substance in the watermark encoder. A watermark extractor or finder includes a two-stage handle. Watermark recovery is the initial step that applies some scrambling calculations to extricate a succession alluded to as recovered watermarks. At that point, in the second step, the inserted watermarks are identified and removed from an associated motion with containing watermarks. The second step regularly requires the examination and correlation of the inconsistent watermark with the first one, and the results could be a few sorts of certainty appraisal showing the closeness between the extricated watermark and the first one.

Encoding is a process which combines a watermark with a digital image. If an image is represented by II, watermark information as W, a security key as K and encoding system as E then watermarked image IW represented as

\[ IW = E(II, W, K) \]

Watermarking Decoder detects watermark. Watermark detection process can be represented as

\[ W' = D(IW, K, ...) \]
Where D is detection process and IW and K are the inputs. Depending upon the inputs it can be of two type blind process and non-blind process.

A. Spatial Domain

Insertion of watermark is done either in spatial or in transform domain. partition of color is utilized to apply spatial watermarking[2]. Along these lines, watermark seems just in one of the color groups and it is difficult to recognize under typical watch. At the point when hues are isolated for printing, the watermark shows up in a split second. Watermarking in spatial domain is basic and has little computational complexities yet they are not strong[1].

LSB method is straightforward and very basic in spatial domain watermarking. In this strategy, slightest noteworthy bits are supplanted to insert the watermark [1]. Security can be improved by utilizing this technique and high limit is likewise given by this strategy. Be that as it may, this technique has a few weaknesses moreover. The implanted watermark can be effectively altered by an aggressor, once he knows the calculation. This calculation can be clarified by a case: Figure 1 demonstrates the 1-bit LSB. The pixel estimation of the host picture is 10111101 and the mystery information is 001. At the point when LSB is connected to this, pixel estimation of the host picture is changed to 10111100 [10]. It can be shown as:

![Fig. 1: 1 bit LSB](image)

**Fig. 1: 1 bit LSB**

**Fig. 2: Block diagram of Generic Watermarking method a) Non-blind Watermarking b) Blind Watermarking**

Security of method can be increased by changing the position of the LSB. Cryptography can likewise be consolidated with LSB system. In this, figure content is made and a key is utilized for installing this content as a part of the host picture. This key distinguishes which bits can be altered for implanting. The opposite of installing procedure is extraction. To recoup the first watermark, the extricated bits can be utilized with cryptography keys [18].

B. Transform Domain

There are a few procedures that depend on change space watermarking [1]. Above all else, have information is changed and alterations are connected to changed information and afterward converse change is connected to get the watermarked picture. It is exceptionally troublesome for an assailant to peruse or adjust the watermark since watermark installed in the change space is unevenly scattered in the host picture [8]. Different systems for watermark are DCT, SVD, and DWT and so forth.

1) Discrete Cosine Transformation

Discrete Cosine Transformation (DCT) changes a flag from the spatial into the recurrence area by utilizing the cosine waveform. DCT isolate the data vitality in the groups with low recurrence and DCT ubiquity in information pressure strategies, for example, JPEG and MPEG. The DCT permits a picture to be separated into various recurrence groups, making it much less demanding to embed watermarking data into the center recurrence groups of the picture. DCT speaks to information as far as recurrence space. DCT based watermarking strategies are powerful when contrasted with spatial area systems. DCT space watermarking can be arranged into Global DCT watermarking and Block based DCT watermarking.

![Fig. 3: Discrete Cosine Transform regions](image)

**Fig. 3: Discrete Cosine Transform regions**

Discrete Cosine transform can be represented as

\[
\text{DCT}(f) = \sum_{n=0}^{N-1} f(n) \cos \left( \frac{\pi}{N} n k \right)
\]

The real advantages of DCT incorporate its high vitality compaction properties and accessibility of quick calculations for the calculation of change. The vitality compaction property of the DCT brings about change coefficients with just couple of coefficients having values, in this way making it appropriate for watermarking. Inserting rules in DCT area are more hearty to JPEG/MPEG.

III. DISCRETE WAVELET TRANSFORM

Watermarking plans in light of DWT are more vigorous. A flag is isolated into two sections: high recurrence and low recurrence. The edge segments of the flag are constrained to high recurrence part. Low recurrence part is further subdivided into high and low frequencies. This process is rehashed a discretionary number of times. Unique flag can be recreated from these DWT coefficients and it is called reverse DWT (IDWT). Picture can be disintegrated into recurrence sub-groups utilizing diverse sort of channels like Haar Wavelet Filter, Daubechies and so forth. Initially level dwt deteriorates the picture into four sub-groups are LL, LH, HL, HH i.e., even points of interest, estimation subtle elements, vertical points of interest and corner to corner subtle elements as appeared in Figure 2.

![Fig. 4: First Level Decomposition](image)

**Fig. 4: First Level Decomposition**
Second level of decay is done on first level LL sub-band of the picture which comes about into another level of deterioration as appeared in Figure 3.

![Second Level Decomposition](image)

**Fig. 5: Second Level Decomposition**

To keep away from the corruption and increment indistinctness of the host picture, watermark is installed in high recurrence sub-groups. Be that as it may, heartiness might be decreased because of implanting watermark in high recurrence sub-groups. Watermark might be inserted in LH and HL sub-groups to enhance execution and heartiness [3]. Saxena et al. proposed a picture watermarking plan which is powerful against various assaults. They utilize DWT and IDWT change to get four recurrence sub-groups. High recurrence sub-band was utilized to implant the watermark [4].

In DWT method, Wavelet coded picture is a multi-determination depiction of the picture. Along these lines, diverse resolutions of a picture can be appeared at changed levels and can be successively prepared from low determination to high determination. However, DWT is computationally more complex as compared to DCT.

IV. SINGULAR VALUE DECOMPOSITION

SVD is a direct variable based math method used to determine numerous scientific issues. It is a heartily watermarking plan for sound signs. SVD has been locked in for various picture applications. For example, pressure, hash extraction and picture watermarking. In picture watermarking applications, the particular estimations of the host picture are adjusted so as to insert the watermark. SVD can proficiently speak to the logarithmic properties of a picture. SVD strategies can be connected to an image. In the event that it is a dim scale picture the lattice qualities are measured as force qualities and it could be altered specifically or changes should be possible subsequent to changing pictures into recurrence space. Particular values in an advanced picture are less influenced if general picture preparing is performed. It implies that for a little bother added to an image, its SVs don’t change fast.

Let A be a general genuine (complex) lattice of request mxn. The solitary esteem deterioration is the accompanying factorization [5]

$$A = U \cdot S \cdot V^T$$

Where, U and V are orthogonal (unitary) and S =diag(σ1, σ2, ...,σr), where σi, i = 1,..., r are the singular values of the matrix A with r = min (m, n) and satisfying:

$$σ_i ≥ σ_{i+1} ≥ ... ≥ σ_r$$

V. NEURAL NETWORK

Neural Network can be characterized as a framework comprises of extensive number of neurons to process data. An artificial neural network can be formulated without making a model of a genuine natural framework. It can be utilized for image investigation, speech processing and so on. It comprises of three layers: input layer, intermediate layer and output layer [7]. These layers are comprised of interconnected neurons. Examples are exhibited to the information layer. This information layer imparts to at least one shrouded layer. In intermedium layer, real preparing is done through weighted associations. Shrouded layer is likewise called kohonen layer as the weights amongst information and this layer is prepared without anyone else's input arranging kohonen run the show. Training set from past examples are used to model the neural network. Training set contains input and outputs. Neural system makes associations and learns designs in view of this information and output sets. Amar et al. proposed an advanced video watermarking plan which depends on fake neural system and multi determination movement estimation. On the premise of relationship between a wavelet coefficient and its neighbor, implanting and extraction of the watermark is finished. Neural system was utilized to recall the connections between coefficients of the image [8].

In view of the preparation, neural system decides computational standards that can be connected to the elements of an image of obscure character [7]. In implanting process, the cover image is provided as contribution to the information layer of the system and weights are changed in accordance with create the comparing target watermark image at the yield layer. Amid extraction of watermark, watermarked image is taken at the information layer and last yield watermark image is created at the yield layer. The yield watermark is connected with the objective yield watermark to decide the PSNR of the got watermark image. Bansal et al. proposed a technique which depends on Back Propagation Neural Network. Fancied watermark image is created via preparing the cover image. The whole prepared neural system weights have been covered up in the host image at the end of the preparation. This makes it conceivable to supply just host image without outer weight records. Amid extraction, weights can be gotten from the host image and prepared neural system can be recreated and it changes over the host image into watermark image. This strategy does not deliver noticeable crumbling of the host image. This technique is secure as it prompts to watermarking in a roundabout way [6].

VI. RSA ALGORITHM

It is utilized for secure information transmission. Lopsided key cryptography is the reason for RSA calculation. Cryptography is utilized for data stowing away and confirmation. Message is covered up as cipher text and afterward watermarking is utilized to implant the message in the image without changing its size or configuration [13]. It is utilized to anticipate unapproved get to sensitive data. In the event that an unapproved individual recoups the watermark, still he can’t get the first watermark and the beneficiary ought to have the capacity to recognize that the message has been adjusted or altered. The upsides of utilizing RSA are that it is straightforward, secure, simple to execute and adjust.

Many methods using RSA have been presented which mix RSA with different transform like DWT and DCT.

VII. ATTRIBUTES OF WATERMARKING TECHNIQUES

A legitimate assessment of watermarking schemes needs to guarantee that all the requirements meet to an assurance level. Each watermarking framework ought to have specific
properties with respect to the given application; in this way, there is no novel arrangement of properties that all watermarking frameworks need to fulfill. By and large, there are five critical issues that are typically considered in the most pragmatic application; they are highlighted below:

A. Reliability

Despite the fact that strength and limit are connected as in plan with high limit are normally simple to annihilation, we trust that it is sufficient to assess them independently. Watermarking plans are characterized for a specific application and every application just requires a specific altered payload so we are just worried by the robustness of the plan for this given payload.

The robustness can be evaluated by measuring the location likelihood of the mark and the bit error rate for an arrangement of criteria that are pertinent for the application which is considered. The levels of rigor range from zero robustness to provable robustness[10,7].

B. Imperceptibility

Imperceptibility is a vital condition for advanced watermarking; that is, the visual similitude between the watermarked form and unique one of the media component and the perceptual nature of the first flag ought to be changed imperceptibly by the inclusion of the watermark. There are two primary reasons why it is essential to keep the indistinctness of the host media after the encoding with watermark information. Firstly, the nearness or absence of a watermark can’t be recognized from the main role of the unique media, if the watermarked media is so severely twisted that its value is lost. Likewise, suspicious noticeable antiques may present a watermark in presence, and maybe its exact area being recognized from host media. This data may give gets to misshaping, substituting, or evacuating the watermark information malevolently. Along these lines, the data inserted in it might never again be accessible.

C. Security

All current watermarking calculations which are not secure can’t be utilized for copyright protection, information verification, or following the unlawful appropriation of computerized substance. Therefore, the watermarking calculation is protected and strong, if the aggressor, utilizing watermarking systems and learning, does not know the key utilized for watermarking advanced substance. Therefore, the concealed watermark data can’t be pulverized or harmed. Likewise, the multifaceted nature of the watermark procedure might be security related in light of the fact that the aggressor will be disheartened to look the addition in an inserting space and long key position. Hence, with a specific end goal to enhance the security of the calculation, it can grow the installed space, and increment the extent of the keys split into little bits of cover image.

D. Capacity

In many applications the capacity will be an altered requirement of the framework so strength test will be finished with an arbitrary payload of given size. While building up a watermarking plan how-steadily, knowing the exchange off between the essential necessities is exceptionally helpful to know and diagram with two changing prerequisites, the others being settled, are a basic approach to accomplish this. In the essential three parameter watermarking model for example one can concentrate on the connection amongst power and quality of the assault when the nature of the watermarked medium is altered, between the quality of the assault and the and the visual quality or between the heartiness and the visual quality [6]. The first is presumably the most vital chart. For a given assault, and a given visual quality, it demonstrates the bit blunder rate as an element of the quality of the assault. The sec-ond one demonstrates the most extreme assault that the watermarking calculation can endure. This is utilized ful from a client perspective: the execution is settled (we need just 5% of the bits to be corrup-ted so we can utilize blunder adjustment codes to recuperate all the data we needed to cover up) thus it characterizes what sort of assaults the plan will survive if the client acknowledges such or such quality debasement.

E. Speed

Speed is extremely subject to the kind of imple-mentation: programming or equipment. In the auto-mated assessment benefit we propose in the following area, we are not worried with equipment executions. For these, the multifaceted nature is an imperative criterion and some application force an impediment on the most extreme number of doors that can be utilized, the measure of required memory, and so forth.

VIII. CONCLUSION

Paper presented a review and utilized a duality way to deal with the watermarking assessment issue by part the assessment criteria into two (free) bunches: usefulness and affirmation. The primary gathering speaks to an arrangement of prerequisites that can be checked utilizing concurred arrangement of tests the second is an arrangement of level to which every usefulness is assessed. These levels go from zero or low to high.

We are researching how evaluation profiles can be characterized for various applications and how significance inspecting systems could be utilized to assess the false alert rate in a computerized way.

Ideally this new era of watermarking testing device (in the continuation of the StirMark benchmark will be extremely valuable to the watermarking group)

REFERENCES


A Review on Digital Image Watermarking and its Techniques
(IJSRD/Vol. 4/Issue 10/2016/119)

Computer Science and Information Technology, pp. 138-142, April 2012.


[10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24] [25]