A Comprehensive Survey of Contemporary Researches in Watermarking for Copyright Protection of Digital Images

Mr.Manjunatha Prasad.R
Assistant Professor
Department of Electronics
K.S.Institute of Technology, Bangalore

Dr.Shivaprakash Koliwad
Professor & Head, Department of Electronics
Malnad College of Engineering
Hassan

Summary
Nowadays, a chief problem encountered by content providers and owners is the protection of their material. They are apprehensive about copyright protection and further forms of exploitation of their digital content. The ease by which digital information can be duplicated and distributed has led to the need for effective copyright protection tools. Diverse techniques including watermarking have been introduced in effort to tackle these increasing concerns. Recently digital watermarking technology has emerged as an effective solution for protecting the digital content from unauthorized copying. A wide variety of watermarking techniques have been proposed by researchers for the copyright protection of digital images. An extensive review of the prevailing literature in watermarking of digital images for copyright protection is presented along with the classification. In addition, a concise introduction about digital watermarking is presented along with its properties, applications and techniques.

Key words:
Digital images, Digital image watermarking, Copyright protection, Ownership, Spatial domain, Frequency domain, Robust, Fragile.

1. Introduction

The drastic development of multimedia content in digital form has escalated the necessity to build secure methods for legal distribution of the digital content. Owing to the rapid advancement of the Internet and multimedia systems in distributed environments, it is now easy for digital data owners to transmit multimedia documents across the Internet. Thus, there is a rise in apprehensions over copyright protection of digital contents [1], [2]. Security of digital images has turned out to be of great significance with the omnipresence of internet. The introduction of image processing tools has resulted in increased vulnerability for illicit copying, modifications, and dispersion of digital images. Besides, the data hiding technologies for digital data like digital watermarking have attracted enormous attention recently [3]. Digital watermarking is deployed so as to prohibit illegal replication or exploitation of digital images [4], [5].

Digital watermarking is a technique that proffers a means to guard digital images from illegal copying and manipulation. The procedure of embedding data into a multimedia element like image, audio or video is referred to as watermarking [6]. It is possible to extract this embedded data at a later stage, or detected in, the multimedia element for diverse purposes including copyright protection, access control, and broadcast monitoring. A digital watermark is an unnoticeable signal added to digital data, known as cover work, which can possibly be identified at a later stage for buyer/seller identification, ownership proof, and the like. Digital watermarking can be categorized into image watermarking, video watermarking and audio watermarking depending upon the range of application. Contemporary digital watermarking schemes chiefly target image and video copyright protection [7]. Commonly, a digital watermark is a code that is embedded within an image. It plays the role of a digital signature, providing the image with a sense of ownership or authenticity. The primary benefit of watermarking is that the content is not separable from the watermark.

A watermark is capable of exhibiting numerous significant characteristics. These comprise that the watermark is hard to perceive, endures common distortions, resists malicious attacks, carries numerous bits of information, is capable of coexisting with other watermarks, and demands little computation to insert or detect [8]. On the outline; an image watermarking procedure needs to satisfy the subsequent requirements [25].

- **Transparency:** The embedded watermark pattern does not visually destroy the original image fidelity and needs to be perceptually invisible.
- **Robustness:** The watermark pattern is hard to detect and remove in an illegal way. In order for a watermark to be beneficial it needs to be flexible to a range of possible attacks by pirates. These attacks may be robustness against compression such as JPEG, scaling and aspect ratio changes, rotation, cropping, row and column removal, addition of noise, filtering, cryptographic and statistical attacks, as well as insertion of other watermarks [9].

Watermarks and watermarking techniques can be divided into diverse categories in a wide range of ways. The watermarking is categorized into Non-blind, Semi-Blind and Blind schemes on basis of the requirements for watermark extraction or detection [10], [11]. Non-blind watermarking schemes identify the watermark with the aid of the original image and secret keys. Semi-Blind techniques demand the presence of both the secret key(s) and the watermark bit sequence. Conversely, the blind techniques require only the secret key(s) for extraction. It is possible for the embedded data (watermark) to be either visible or invisible. In case of visible watermarking of images, a secondary image (the watermark) is embedded in a primary image in such a way that watermark is intentionally detectable to a human observer while in the case of invisible watermarking the embedded data is not detectable, but can possibly be extracted by a computer program [12].

Robust watermarking is commonly designed to resist un-malicious or malicious attacks like scaling, cropping, lossy compression, and the like. Robust watermarking is chiefly focused on copyright protection. On the contrary, fragile watermarking is intended to identify any tiny modification to the original digital content [13]. Fragile watermarking was employed to decide on if the image has been altered or not. It is possible to authenticate the integrity of the images with the aid of a fragile watermark. An simple example of a digital watermark would be a visible “seal" placed on an image to identify the copyright owner (for example [20]). A visible watermark is restricted in many ways. It inscribes the image fidelity and is vulnerable to attack through direct image processing. A watermark needs to possess the following features in order to be effective [66]:

1) **Unobtrusive:** The watermark needs to be perceptually invisible; in other words its presence must not hinder with protected work.
2) **Robust:** The watermark needs to be tedious (impossible; to be precise) to remove. When only incomplete knowledge is present (for instance, the precise location of the watermark in an image is unknown) then attempts to remove or demolish a watermark, should consequent in severe degradation in fidelity prior to the loss of the watermark. Especially, the watermark needs to be robust to [66]:
    a. **Common signal processing** - It is necessary that the watermark be retrievable despite common signal processing operations being applied to the data. These operations may be one among the following: digital-to-analog and analog-to-digital conversion, re-sampling, re-quantization (including dithering and recompression), and common signal enhancements to image contrast and color, or audio bass and treble.
    b. **Common geometric distortions** (image and video data) - Watermarks in image and video data need to be resistant towards geometric image operations such as rotation, translation, cropping and scaling as well.
    c. **Subterfuge Attacks: Collusion and Forgery -** Additionally, the watermark must be flexible to collusion by multiple individuals each possessing a watermarked copy of the data. In other words, the watermark needs to be robust to combining copies of the same data set to destroy the watermarks. Moreover, when a digital watermark is to be employed in litigation, it should be impractical for colluders to merge their images to produce a different valid watermark with the objective of framing a third-party.
3) **Universal:** The same digital watermarking algorithm needs to be applicable for all three media under consideration. This is potentially helpful in the watermarking of multimedia products. This feature is favorable for the implementation of audio and image/video watermarking algorithms on common hardware as well [66].
4) **Unambiguous:** Retrieval of the watermark must unambiguously recognize the owner. In addition, the precision of owner identification needs to degrade gracefully in the face of attack [66].

The storage, access and distribution of digital images have developed a lot owing to the innovations occurring in the field of information and communication technology [14]. With the exceptional raise in the necessity for sharing digital images, the requirement of copyright protection as well has grown proportionally. In this paper, we have presented an extensive review of the significant researches associated with the digital image watermarking for copyright protection. A brief discussion about the general concepts associated with the digital watermarking is presented. In addition the properties of watermarking, watermarking applications and digital watermarking for copyright protection are detailed as well.

The paper is organized as follows: The properties of watermarking are detailed in Section 2. In section 3 watermarking applications are presented. A brief introduction to digital watermarking for copyright protection is presented in Section 4. Extensive reviews on the study of research techniques for digital image watermarking and copyright protections are provided in Section 5. The conclusions are summed up in Section 6.

2. Properties of Watermarking

Watermarking systems can be characterized through a number of properties [15], [16]. The relative importance of each property depends on the requirements of the system application. The properties discussed in this section are related to watermark embedder, watermark detector, or both.

2.1 Embedding Effectiveness

The efficiency of a watermarking system lies in the prospect that the output of the embedder will be watermarked. When input to a detector result in positive detection the cover work is believed to be watermarked. It is possible to determine the effectiveness of a watermarking system analytically or empirically by embedding a watermark in numerous cover works and identify the watermark. The proportion of cover works that produce positive detection will be the probability of effectiveness [15].

2.2 Fidelity

Commonly, the reliability of a watermark system refers to the perceptual resemblance between the original and the watermarked version of the cover work. Nevertheless, it is possible for the watermarked work to be degraded in the transmission process earlier to it being seen by a person, a different definition of fidelity might be further suitable. It is possible to define watermarking system fidelity as a perceptual similarity among the un-watermarked and watermarked works at the point at which they are offered to a viewer [16].

2.3 Data Payload

Data payload denotes the number of bits a watermark embeds in a unit of time or works. In case of audio, data payload denotes the number of embedded bits per second that are transmitted. Diverse applications demand diverse data payload. For instance, Copy control applications may necessitate a few bits embedded in cover works [15].

2.4 Blind or Informed Detector

We denote the detector which necessitates the original, un-watermarked work as an informed detector. There is a possibility for the informed detectors to demand for information obtained from the original work rather than original work itself. Conversely, detectors that do not require the original work are referred to as blind detectors. Informed detector provides an enhanced performance in watermark extraction. Nevertheless, this might lead to an enormous number of original works being stored [16].

2.5 False Positive Rate

A false positive is the identification of a watermark from a cover work which does not contain one in reality. When we speak about a false positive rate, we denote the number of false positives we anticipate to happen in a given number of runs of the detector.

2.6 Robustness, Security and Cost

Robustness denotes the capability to detect the watermark after common signal processing operations. Audio watermarking should robust to temporal filtering, A/D conversion, time scaling and the like. Not all applications of watermarking demand all the sorts of robustness. This depends on the nature of application of watermarking system [15], [16]. The security of a watermark denotes its capability to oppose aggressive attacks. Hostile attack is the process specifically intended to thwart the watermark's purpose. Unauthorized removal, unauthorized embedding, and unauthorized detection are the three chief categories of attacks. The Cost of watermarking system denotes the speed with which embedding and detection needs to be carried out and the number of embedders and detectors that need to be employed.

3. Watermarking Applications

Watermarking applications have been briefly summarized in this section. In a few words, these applications can be classified following the general consensus on digital media watermarking [15], [16].

- **Copyright Protection** - Watermarking is essentially applied for copyright protection. The aim is to evade other parties from claiming the copyright by embedding the information that identifies the copyright owner of the digital media. The application must make certain that embedded watermark cannot be eliminated without causing a noteworthy deformation in digital media through maintaining a high level of robustness. It is important to consider further necessities in addition to robustness. For instance, the watermark must ably determine rightful ownership if other parties embed additional watermarks and also explicit by nature.
- **Signatures** - The content owner is recognized by the watermark. It is possible that this might be exploited by a potential user to get hold of legal rights to copy or publish the content from the contact owner.
- **Fingerprinting** - Watermarks can be employed to recognize the content buyers. This might be of

great assistance in tracing the source of illegal copies.

- **Broadcast and publication monitoring** - In case of signaturing, the watermark identifies the owner of the content whereas here it is detected with the aid of automated systems that monitor television and radio broadcasts, computer networks, and other distribution channels to monitor when and where the content appears.
- **Authentication** - At this juncture, the watermark encodes information essential to conclude that the content is authentic.
- **Copy control** - The watermark comprises of information regarding the rules of usage and copying which the content owner desires to enforce. These will commonly be undemanding rules like “this content may not be copied”, or “this content may be copied, but no subsequent copies may be made of that copy”.
- **Secret communication** - The embedded signal is employed in the transmission of secret information from one person (or computer) to another, devoid of anyone along the way becoming aware that this information is being transmitted [16].

4. Digital Watermarking for Copyright Protection

Copyright protection seems to be one of the first applications digital watermarking was intended towards. Here, the metadata comprises of information regarding the copyright owner. It is unnoticeably embedded as a watermark in the cover work that is in need of protection. . When users of digital content (music, images, and video) possess an easy access to watermark detectors, they need to be capable of recognizing and interpreting the embedded watermark and identifying the copyright owner of the watermarked content.

Digimarc Corporation’s [83] Image Bridge Solution is one example of a commercial application built for this purpose. The Image Bridge watermark detector is made accessible in the form of plug-ins for numerous accepted image processing solutions including Adobe Photoshop or Corel Photo Paint. As soon as a user opens an image with the aid of Digimarc enabled application, Digimarc’s watermark detector will identify a watermark. In that case it will contact a remote database with the watermark as a key to locate a copyright owner and his contact information. It is possible for an honest user utilize that information to contact the copyright owner to request permission to make use of the image.

The Digimarc Corporation has illustrated the way in which an invisibly embedded watermark can be employed to identify copyright ownership. It would be beneficial if an embedded watermark could be employed to prove the ownership as well, possibly even in a court of law. We can imagine the following scenario: Consider a copyright owner distributing his/her digital content with his/her invisible watermark embedded in it. When copyright ownership dispute arises, a legal owner needs to be capable of proving his ownership by indicating that he owns the original work, and that the disputed work has been obtained from the original by embedding a watermark into it. This could be carried out through the production of the original work along with the watermark detector, and making detector identify the owner’s watermark in a disputed work. Regrettably, it seems as though the aforesaid scenario can be defeated under certain assumptions, and owing to that watermarking has not been recognized yet as a technology reliable enough to be employed in proving ownerships.

A considerable issue lies with the availability of watermark detector. It is established that when a detector is extensively accessible it is highly impossible to protect watermark security. Precisely, if a detector is available, there is always a possibility for an embedded watermark to be removed. It is achieved by frequently making undetectable changes to the watermarked work, until a watermark detector becomes unsuccessful in detecting the watermark. If the watermark is removed, the original owner cannot establish his ownership any longer. Even otherwise, Craver et al. [17], [18], [19] illustrated that, under specific conditions, another watermark can be added to a previously watermarked image in such a way as to make it appear that this second watermark is present in all copies of doubtful image, including the original image. This is referred to as an ambiguity attack, and it could be employed not only in disputing the ownership claims of the rightful copyright owner, but as well to create new ownership claim to the original digital content.

5. Comprehensive Review of Recent Researches

Watermarking digital media has received a great interest in the research community. In this section we have presented a comprehensive review of significant watermarking schemes for copyright protection. Most watermarking schemes focus on image and video watermarking and very few focuses on audio. The reviewed watermarking algorithms are classified and described in the following subsections.

5.1 Digital Image Watermarking Techniques

Watermarking is not a new phenomenon. In the modern era, proving authenticity is becoming increasingly important as most of the world's information is stored as readily transferable bits. Digital watermarking is a process whereby arbitrary information is encoded into an image in such a way that the additional payload is imperceptible to the image observer [21]. Watermarking algorithms available fall into two categories. Spatial-domain techniques work with the pixel values directly. Frequency-domain techniques employ various transforms, either local or global. Several widely recognized techniques are described subsequently [22].

5.1.1 Spatial Domain Methods

Mahfuzur Rahman and Koichi Harada proposed a method to embed information in objects with layered 3D triangular meshes such as those reconstructed from CT or MRI data, a parity enhanced topology based spot area watermarking method [21]. The robustness against unauthorized alteration of a single bit in every consecutive 8-bits of length is enhanced by the incorporation of parity checking. Watermark message is cut into numerous pieces and each piece of message is embedded at different spots, hence, if a piece of message is lost in one spot, the error correct decoding can be employed to possibly retrieve the same information from other spots. Simple, effective, computationally faster, and inexpensive were the traits of their proposed method. Their method acted against unintentional attacks translation, rotation, arbitrary re-sectioning, scaling etc, and left artifact after intentional attacks of local and global number re-arrangement in a robust manner. The method had the ability to check alteration of a single bit in every consecutive 8-bits length as it is parity enhanced. The applications such as important data identification, detection of change of data, content labeling, ownership assertion, etc. of layered 3D triangular mesh models found their method to be appropriate. The watermarking of geometry sensitive 3D triangular mesh model can be effectively performed by their proposed method.

A fragile watermarking scheme, designed for color image particular object's authentication was presented by Hamad Hassan and Gilani [22]. For instance when a painting is considered, the artist's signature would be principal for us in verification against any sort of processing. Color images with company monogram, institute logo or building name board fall under an identical category as well. Initially the color image provided is transformed from RGB to YST color space. The new color space is exclusively designed for watermarking the color media by Francesco et al. [23]. The T channel is analogous to the chrominance component of a color image and YS $\perp$T, thus, the T channel is explicitly chosen for embedding the watermark information. Once the color space transformation is carried out, the T channel is divided into 2×2 non-overlapping blocks and two LSBs of each block are set to zero. The object of an image that needs to be authenticated is as well partitioned into 2×2 non-overlapping blocks once essential resizing is carried out. This is followed by the computation and encoding of intensity mean of each block of object up to eight bits to enclose the watermark information about each block of object. Following the watermark generation, secure mapping of blocks of the T channel is produced on basis of 2D-Torus Automorphism presented by G. Voyatzis et al. [24] with the aid of a private key. The block information of the object of interest (each block) is then embedded into the mapped block's LSBs. Later, the embedded watermark aids not only in the authentication of work but also in the full recovery of original work. The scheme proposed them is capable of accurately localize the tampering in the object under consideration besides recovering it with a probability of almost one.

Xiangui Kang et al. [25] have modeled the data extraction process as one associated with a generalized channel of additive noise with a generally non-zero mean and fading by adaptively estimating the decision zone exploiting a training sequence and estimating the quantization step size using the Fourier analysis method. Thus, predominantly, the robustness of the watermarking system against median filtering, intensity DC change, color reduction, intensity linear scaling, non-linear intensity modification such as Gamma correction etc is improved. Their approach functions against common signal processing including Gaussian filtering, mean filtering, median filtering, sharpening, and JPEG compression with a quality factor of as low as 10, robustly. The chief progress is the enhanced robustness against median filtering, intensity DC change, intensity linear scaling, color reduction, histogram equalization and intensity non-linear scaling, etc. in comparison with the watermarking scheme described in [28] which does not employ adaptation. The proposed scheme attains much superior robustness to additive noise corruption, JPEG compression, median filtering, and accomplishes much enhanced watermark invisibility simultaneously in comparison to the scheme proposed in [27] which employs a training sequence as well. The robustness of their proposed adaptive estimation of the decision zone can be enhanced by combining with many existing watermarking schemes [26], [28].

Lu et al. developed a cocktail watermarking scheme for digital image protection [29]. The embedding of two complementary watermarks which makes it difficult for attackers to destroy both of them and lower bound provided for the cocktail watermarking by the statistical analysis are the two characteristics of their scheme. They illustrate the robustness of their watermarking scheme even as the typical watermarking requirements are satisfied through the results. The applicability of this scheme to other types of media such as audio [33] or video is an additional significant feature of their cocktail watermarking technique. The authors while maintaining comparable robustness have also enhanced this non oblivious cocktail watermarking scheme to form an oblivious one [34]. The important issues such as the rightful ownership deadlock problem [17], the capacity problem [32], [35] and the public-key detection problem [31] will be considered in future research in addition to the robustness issue of watermarking addressed in their paper.

Lu et al. presented a multipurpose watermarking scheme which can be applied to attain both authentication and protection of multimedia data [2]. The hiding process embeds the watermark once which can be extracted for diverse applications in the detection process, invisibly. a) The approximation information of a host images kept in the hiding process by utilizing masking thresholds defined based on the human visual system. b) Oblivious and robust watermarking accomplished. c) An asymmetric robust range adopted for fragile watermarking to achieve malicious tampering detection and non-malicious tampering tolerance are the three special features of their proposed scheme. The authors intend to verify data integrity as well to confirm the rightful ownership employing this multipurpose watermarking scheme. The extreme efficiency of their watermarking scheme for content authentication and copyright protection is illustrated by the results. The authors extended the method to audio watermarking besides images (gray-scale and color).

A novel watermarking system based on the principles of informed coding and informed embedding was presented by Miller et al. [37]. About 1380 bits of information in images with dimensions 240 × 368 pixels can be embedded by their system. The robustness of the watermarks against momentous volumetric distortions, including additive noise, low pass filtering, contrary changes and lossy compression is illustrated through the experiments performed on 2000 images. In their system, watermark messages are encoded with the embedded signal selected according to the cover image using a modified trellis code in which a given message may be represented by a variety of different signals. It is made certain that the message will not be confused with other messages even after addition of noise as the signal is embedded by an iterative method. A perceptual shaping is integrated into the embedding process to enhance fidelity. The considerable enhancement in performance owing to these three components is illustrated.

Lu et al. presented a digital watermarking technique and intended to solve some important issues in the digital world, such as copyright protection, copy protection, and content authentication through their extensive research [38]. They presented an efficient multipurpose watermarking algorithm based on mean-removed vector quantization (VQ). Their algorithm utilizes the robust watermarking method based on index properties to embed the robust watermark in the mean index [39] and a simple index constrained method to embed the fragile watermark in the residual index. There is not much difference in the variance of neighboring mean indices even if the encoded indices of the attacked watermarked image may be very different from the original ones. This leads to the robustness of the watermarking method. In contrast, the residual watermarking method modifies the index in proportion to the bit to be embedded on the basis of an index constrained codeword search procedure. The extracted watermark bit changes owing to any change in the encoded residual indices. Explicitly, it is fragile to most intentional attacks as their watermarking can endure few modifications.

Ruizhen Liu and Tieniu Tan presented a new watermarking method for digital images [40]. The SVD domain of the original image is added with the watermark. The mathematical background of their method is very apparent and the estimation of the error between the original image and the watermarked image was performed. SVD uses non-fixed orthogonal bases which is a one-way non-symmetrical decomposition contrasting to several other unitary transformations which adopt fixed orthogonal bases (such as discrete Fourier transform, discrete cosine transform etc.). The performance of this novel algorithm is good in terms of both security and robustness owing to these properties. Moreover, their algorithm can resolve rightful ownership devoid of encryption and if combined with encryption, they can provide more powerful security for rightful ownership. They performed extensive experiments and employed Cox method [52] for comparison. The robust nature of the novel method against image distortion and its significant superiority over Cox method was illustrated by the results.

Wei Lu and Hongtao Lu [41] provided a novel robust digital image watermarking scheme with the aid of sub-sampling and nonnegative matrix factorization. Originally, sub-sampling is employed to create a sub-image sequence. Later, the nonnegative matrix factorization (NMF) is applied to decompose the sequence on basis of the column similarity of the sub-image sequence. A Gaussian pseudo-random watermark sequence is embedded in the factorized decomposition coefficients. Owing to the high resemblance of sub-images and meaningful factorization for NMF, the proposed scheme is capable of achieving superior robustness, particularly towards common permutation attacks. Experimental evaluation demonstrates the enhanced performance of the proposed scheme.

An innovative digital watermarking method that works on basis of vector quantization (VQ) was projected by Chin-Chen Chang and Hsien-Wen Tseng [42]. On contrary to the traditional VQ-based watermarking schemes, the mean of sub-blocks is employed to train the VQ codebook. Besides, the Anti-Gray Coding (AGC) technique is utilized to improve the robustness of the proposed watermarking system. Here, the secret keys are employed to conceal the related information between the original image and the watermark followed by the registration of a set of secret keys to a trusted third party for future confirmation. Therefore, the original image stays unaltered even after the watermark being melted into the set of secret keys. Experimental evaluation illustrates that the watermark is capable of surviving a range of possible attacks. Moreover, the size of the secret keys can be reduced as well.

The foremost limitation for numerous watermarking methods is the geometric distortions. An answer to the common problems of rotation, scale, and translation is presented by Lin et al. [43]. Their solution and the prior proposals in the pattern recognition literature regarding invariants of the Fourier–Mellin transform are associated. Nevertheless, they do not unambiguously derive an invariance relationship, which is contrasting with those proposals. They generate a signal that changes in a trivial manner as a result of rotation, scale, or translation rather than generating a truly RST invariant signal. The Fourier transform of the image is taken and a log-polar re-sampling is performed and then integrated along the radial dimension in order to calculate this projection. They observed that the Radon transform can be employed for alternative implementation [44].Their technique is resilient against mild JPEG compression as well. A function of the probability of false positive determines the change in the degree of resilience. In addition, the inefficiency of their method against cropping, an attack against which no steps have been taken in the design has been illustrated through the results.

5.1.2. Frequency Domain Methods

The discrete wavelet transforms (DWT) and the discrete cosine transform (DCT) have been implemented effectively in numerous digital image watermarking. Ali Al-Haj [45] demonstrated a combined DWT-DCT digital image watermarking algorithm. Watermarking was carried out through the embedding of the watermark in the first and second level DWT sub-bands of the host image sub-sequenced by the application of DCT on the selected DWT sub-bands. The blend of the two transforms enhanced the watermarking performance by a great deal on comparison with the DWT-Only watermarking approach. As a concluding remark, the combination appropriate transforms with the DWT in DWT-based digital watermarking applications, might possibly have a positive influence on performance of the watermarking system.

Muhammad Shafique Shaikh and Yasuhiko Dote [46] utilized a watermarking technology which worked on discrete wavelet transformation and employed a random and a text watermark for testing. The watermarks consequently embedded were established to be perceptually non-obstructive on six different gray level images and an mpeg color video. A comparison of the proposed work with an earlier work was carried out and the results were found to be encouraging. The watermarks were extracted from noisy images to a satisfactory degree of correlation for every gray scale image. Maximum correlation was attained for the type image and result was found to be consistent with all four noises. Upon comparison of the noises, highest correlation coefficient, ρ, is attained for the case of Gaussian noise with ρ greater than 0.96 in most cases and with irregularities in the distribution at smaller SNR of les 47.0 dB. . For SNR higher than 50.0 dB, there is not much deviation in ρ for all images. The shape of the distribution is found to be further regular for other noises at all values of SNR with ρ greater than 0.5. They tested the illustrated watermarking method with an mpeg color video consisting of 30 frames as well. The watermarks embedded with the aid of the proposed schemes were found to be undetectable on visual inspection of individual frames and video. Thus, it is possible for them to safely state that in case of gray scale images the proposed method has survived with the additive Gaussian, salt and pepper, Speckle, and JPEG noises of different intensity for the selected host images and random and text watermarks and besides, it has as well sustained the degradation due to Gaussian, salt and pepper, and Speckle noises of the adopted range on mpeg color video with the aid of random watermark.

The DWT-SVD method that merges the SVD technique with the DWT method is found to be more robust than the DWT-based method. However, the DWT-SVD method as well retains the disadvantage of the SVD method and so it is not found to be tough against cropping attacks. With the intention of satisfying the security obligations for copyright protection, Jung-Chun Liu et al. [47] projected a multi-scale Full-Band Image Watermarking scheme by merging both of the DDWT-based and the SVD-based techniques. They make use of both of the advantages of the DDWT method like robustness against cropping attacks, and that of the SVD method including robustness against geometric attacks like rotation and scaling and non-geometric attacks for example Gaussian noise, sharpening, and contrast adjustment. Results illustrate that the multi-scale Full-Band Image Watermarking scheme is further robust than the DWT-SVD method.

A technique for embedding a watermark into a color image by coding and synchronization of coefficient-value peak locations in the DFT domain was projected by Yen-Chung Chiu and Wen-Hsiang Tsai [48]. In accordance with the characteristics of the image coefficients in the DFT domain, they embed the watermark through creation of peaks circularly and symmetrically in the middle frequencies. Additionally, they employed a combinatorial operation to code the peak locations. Furthermore, the synchronization of the peak locations was carried out by a supplementary synchronization peak. In the watermark extraction procedure, the positions of the coefficient-value peaks are identified and mapped into a combinatorial operation in order to obtain a watermark. The embedded watermark is illustrated to be robust and capable of surviving print-and-scan operations. Their method is capable of accomplishing the objective of protecting the image copyright of the owner. Nevertheless, by their watermark embedding technique, the capacity of a normal-size image is not adequate enough for hiding a common logo image.

A DCT domain based removable visible watermarking algorithm that moderately succeeds in defeating illegal removal and resisting compression was presented by Yang et al. [49]. They intended to protect the multimedia content and to ensure that the reconstructed images are of high-quality for authorized users, or else, of low-quality for unauthorized users by embedding the visible watermark. Their method enabled preventing the embedded visible watermark from being illegally removed by unauthorized users without correct user keys as their proposed scheme preprocesses the watermark using a secret key before embedding it into host images which is in contrast to the existing approaches that directly embed watermarks into host images. A mathematical model that utilizes the HVS features was established to determine the adaptive scaling and embedding factors. Furthermore, this mechanism can be applied to other transform domains by easy extensions of the method. Integer transform can be utilized to implement Lossless recovery as it avoids rounding error.

Digital watermarking can be robustly implemented utilizing Singular Value Decomposition (SVD), one of the best transforms for this purpose. In several SVD based watermarking techniques, the Eigen-values of the cover image are embedded with Eigen-values of the watermark and the key parameter employed is the eigenvectors. Owing to the fact that the original eigenvectors have been used in extraction process, this group of methods is not proficient to offer the secure watermarking technique. Azadeh Mansouri et al. [50] presented two new secure methods of non-blind image watermarking. They employed modification on singular values of the host data by embedding DCT coefficients of the watermark image to implement the two methods. These coefficients of watermark are employed as the information which is embedded to provide the secure schema owing to the pleasant properties of DCT in the form of a reversible transform, and consideration of the advantages of same variation as the Singular values change. Rather than changing the local variation of the signal, just the brightness can be altered to achieve the best quality for watermarked image, moreover enough robustness against large amount of attacks.

Fangjun Huang, Zhi-Hong Guan et al. [51] presented a novel method for embedding digital watermark which combines the singular value decomposition (SVD) and the discrete cosine transform (DCT) into the original image. In this method, only the singular values (SVs) of a recognized pattern need to be embedded into the original image to easily obtain more transparency. In addition, their method achieves the highest possible robustness without degrading image quality and losing the transparency by adopting LPSNR.

The idea of using spread spectrum for embedding watermarks in the discrete cosine transform (DCT) domain was invented by Cox et al. [52]. The method considers the host image and the watermark to be a communication channel and a signal to be transmitted, respectively. The perceptually important part of the signal spectrum is spread with the watermark message. Gaussian-noise like watermarks is employed to accomplish security. The watermarked image will be damaged if an attempt is made to destroy the watermark. Since the original image is required for watermark extraction, it is not a blind watermarking scheme. The watermarks can be embedded in wavelet coefficients for images as well as video using the spread-spectrum method, in general [53].

Langelaar and Langendijk proposed a method called differential energy watermarking (DEW) [54]. A macro block which composes of several 8x8 DCT blocks is embedded with a watermark bit by dividing the block into two parts. In order to produce an energy difference in the two parts of the same macro block, where the energy difference is determined by the watermark bit, the High-frequency DCT coefficients in the compressed bit stream are selectively discarded. The number of 8x8 DCT blocks in a macro block, JPEG quantization step size, and a minimal cutoff index for watermarking are the three parameters in this method. Suitable marking systems are obtained for different applications by adjusting the three factors. In case of attacks such as pixel shifting and Stir Mark, the method exhibits a good performance [55]. In addition, the method can be applied in real-time processing as the embedding process is done in the compressed domain.

A watermarking technique to embed an invisible signal into multimedia data so as to attest the owner identification and discourage the unauthorized copying has been proposed by Wu and Hsieh [56]. They proposed a proficient DCT based watermarking technique. Their proposed method embeds the watermark into image and extracts the watermark from the watermarked image more efficiently by exploiting the zero-tree in the rearranged DCT coefficients. Their method is reasonable to employ it in a real time system as it can directly extract the embedded watermark from the watermarked image devoid of the original image. In addition, they offer robust digital watermark by employing a scheme for spreading the watermarking information. The certainty of imperceptibility and robustness of the digital watermark is illustrated through the results.

5.1.3. Other Researches

An adaptive image watermarking algorithm was projected by Chang-Hsing Lee and Yeuan-Kuen Lee [57]. The watermark adopted here is a visually meaningful image so that human eyes can effortlessly judge the extraction result. To embed a watermark in the host image this approach makes use of the sensitivity of human visual system to adaptively alter the contents of a set of blocks. Results demonstrated that their algorithm is robust to common image processing operations like low-pass filtering, median filtering, resampling, requantization and lossy JPEG compression.

Reuse centric system design, artifact watermarking, and cryptography are the existing works that motivate watermarking-based protection of hardware and software design IP. The fundamental precepts, a canonical technique and example applications for watermarking-based IPP were described by Andrew B. Kahng et al. [58]. The thoughts such as: a) Stages of the (hardware, software) design process can typically be viewed as (difficult) optimization instances whose solutions constitute IP to be protected, b) IP watermarking can typically be achieved by adding constraints (e.g., interpreted from a cryptographically secure encoding of the IP owner's signature) to any given design optimization instance, c) The addition of constraints can typically be achieved using pre- or post processing of the inputs and outputs, respectively, for a given design optimization are the key ideas put forth by the authors. Consequently, the watermarking is not intrusive as it often transparent to existing algorithms and tools. The other aspects of watermarking context, e.g., protection requirements against typical forms of attack and cryptography background (one-way functions, cipher streams, and digital signatures) have been analyzed by the authors. Besides, in order to embedding design watermarks at the physical-design level, the authors developed the first IPP protocols. They used leading industrial tools to implement these protocols evidently to existing design flows. The superiority of their method with very acceptable cost overhead for the watermarking and no impact on layout area (given the fixed-die context) or timing was proved in case of real designs. In addition, the robustness of their watermarking scheme against the random tampering attacks was illustrated.

Furon and Duhamel [59] presented the concept of asymmetry in watermarking. Their technique can be tailored to a large number of watermarking techniques based on DSSS, hence its flexibility. Alternatively, the merits of their method in the copy protection framework were analyzed. The description of the targeted application, analysis of the possible threats, and followed by the estimation of the complexity of each class of attacks were their intent. The security level of the watermarking technique offered to the global copy protection system was defined. According to the authors, a watermarked content only attack is not possible with this method whereas it is a real threat for direct-sequence spread spectrum (DSSS) and Watermarking Costa's Schemes (WCS) schemes. A brute force attack of size O (2^L) is necessary for a known cover content attack while it is theoretically possible to disclose the secret key in DSSS techniques with a single pair of watermarked / original content. T. Kalker [60] proves O (N) tries are sufficient for DSSS techniques in contrast to the oracle attack that needs O (N^2) tries. The asymmetric detectors require more complexity, more memory and they accumulate a bigger amount of content in order to take a reliable decision, paying the larger length of the vectors as the price.

5.2. Watermarking Techniques for Copyright Protection

Recent years have seen a rapid growth in the availability of multimedia content in digital form. A major problem faced by content providers and owners is protection of their material. They are concerned about copyright protection and other forms of abuse of their digital content. An extensive review of recent researches on watermarking techniques for copyright protection is provided below.

5.2.1. Spatial Domain Methods

A new approach for watermarking polygonal lines was presented by Xu Zhou et al. [61]. GIS data or contour maps can apply their algorithm. It is essential and significant to protect the copyright of such map data as it is very valuable. Even other kind of vector graphics composed of polygonal lines find this approach to be appropriate. Instead of correlation based algorithm, they adopt the hypothesis test detection algorithm based on likelihood ratio test as they embed watermark data by multiply operation. The approach can resist common geometric transform (attacks) owing to its geometric nature. The algorithm is not robust enough to the vertex removal (polygonal line simplification) or addition operation, which can be said as a dearth in the algorithm. Such problem is more easily solved when original data are involved, however, the security of the original data must be significantly destabilized.

In order to overcome the weaknesses of contemporary symmetric watermarking methods, an asymmetrical watermarking method for copyright protection that satisfies the zero knowledge principle was designed by Jengnan Tzeng et al. [62]. All of their watermarking, apart from the secret matrices G and H, have been released and are publicly accessible. Their asymmetric design is robust owing to the fact that it improves the watermark space concept of their preceding symmetric watermarking method. Since their watermark is greatly reliant on the original image, it is not possible to remove it without perceptually distorting the watermarked image. Their method is safe, in view of the fact that they embed secret information Gw inside a subspace of w and present the public with a key $(D = G^T + BH^T)$ to detect Gw. Since the secret basis of G is concealed from the public, approximating Gw is exceedingly tedious.

A concept which is a solution with a specific focus on preventing disputes that comes out of ownership claims through buying and selling digital documents is presented by Yamuna Govindarajan and Sivakumar Dakshinamurthi [63]. The concept aids in authenticating sellers and buyers of digital documents by its reliable watermarking method. Security is also compromised by the employment of public and private keys of owners and buyers as watermarks. The difficulties out of deciphering the public-private keys of the party involved would cause cascading terrible consequences if the encryption technology implemented is tattered. Thus, the hash value derived from the original document and encrypted using only the public key of the owner was selected to watermark in their proposed watermarking method. In order to decrypt the watermark, the knowledge of the private key of the owner is necessary. In addition the public key of the watermark, undeniably associated to the owner is not only unique, but it is registered from a registering authority as well. The proposed concept imprints the hash value derived from a combination of the public keys of the buyer and the owner to solve the Copyright Infringement issues. Others cannot legally claim the public keys as it is necessary to register the public keys with a registering authority after receiving it from the certificate authority. The issues related to buyer-owner identification, copyright infringements and Ownership Dispute Attack can be solved with the aid of this concept.

Wavelet tree based watermarking algorithms approach copyright protection and ownership verification using the wavelet coefficient energy difference. WTQ (Wavelet Tree Quantization) algorithm is the representative technique applied for watermarking, which utilizes energy difference. A new differential energy watermarking algorithm based on the wavelet tree group modulation structure, i.e. WTGM (Wavelet Tree Group Modulation) was presented by Min-Jen TSAI and Chang-Hsing SHEN [64]. The wavelet coefficients of host image are separated into disjoint super trees (each super tree containing two sub-super trees). The group strategy such that energies of sub-super trees are close is utilized to embed the watermark in the relatively high-frequency components. The demerits of the WTQ scheme, insecurity is proficiently enhanced by the utilization of wavelet tree structure, sum-of-subsets and positive/negative modulation. The visual effect of the watermarked image is superior owing o the integration of the HVS (Human Visual System) for WTGM. The efficiency of their algorithm with respect to robustness and imperceptibility is illustrated through the results.

Ming-Chiang Hu et al. intended to achieve the copyright protection through the proposed two-phase watermarking scheme which extracts both the grayscale watermark and the binary one from the protected images [65]. Primarily, their method constructs a grayscale watermark image using the pixel values of the original image. Subsequently, the just-procured-permuted grayscale watermark from the first phase is employed to further retrieve a binary watermark image. Here, a lossless embedding is the outcome of their proposed technique, i.e. the protected images and the original ones are identical. The original image is not necessary in the overall verification procedure. The grayscale and binary watermarks in sequence can be extracted by only those who have the original grayscale watermark and the corresponding secret keys. Therefore, the security and robustness of the proposed watermarking system is improved. In accordance to the results obtained, the general requirements of image watermarking are satisfied by their proposed system and the system is better with respect to transparency and robustness when compared with the related works. In addition, rather than transform-domain techniques, implementation is easier. Hence, their proposed method is more feasible and practical for copyright protection owing to its flexible characteristics.

Hernandez and Perez-Gonzalez addressed the problem of the performance analysis of image watermarking systems that do not require the availability of the original image during ownership verification [66]. The statistical analysis of image watermarking algorithms in which the original image is not needed during the watermark detection and extraction processes was discussed by the authors. In their framework, watermarking is visualized as a communication problem in which a signal carrying some information is transmitted through a noisy channel where the noise is the original image itself which the receiver is unaware of. Therefore, watermark verification can be perceived like a statistical decision problem that involves two tests, namely, detection of the very presence of the watermark and the estimation of the information it can optionally carry. The development of adequate embedding and detection algorithms is precisely based on a careful theoretical analysis of watermarking techniques using a statistical approach formed in both the cases. Besides, in the authors' view, to acquire a better understanding of the different problems that arises in watermarking and to assess rigorously the suitability of different algorithms, considering the performance requirements of copyright protection applications, a theoretical analysis is very essential. Considering the abovementioned requirements, they focused on spread spectrum techniques and analyzed how the overall performance of the system is influenced by how image characteristics, different kinds of attacks, and system parameters such as the length of the bit string carried by the watermark.

A watermark method based on visual cryptography was proposed and the features of their proposed method were summarized by Rawan I. Zaghloul and Enas F. Al-Rawashdeh [67]. A color image (HSV scheme) is employed as the host image. It is not possible to retrieve the watermark pattern from other comparable image. The watermark image is alike the original image as the watermark is not embedded into the original image. The robustness of the method against geometrical attacks like rotation, flipping, cropping, scaling, and shearing has been proved. The robustness of their method against signal processing attacks like noise addition, filtering, and jpeg compression having good Corr values is illustrated.

Ming-Shi Wang and Wei-Che Chen [68] presented a digital image copyright protection scheme based on visual cryptography (VC) and singular value decomposition (SVD) techniques. Their scheme initially applies SVD to a host image to construct a master share. Subsequently, the two-out-of-two VC scheme is used as the basis for constructing an ownership share by the joint utilization of master share with a secret image. The master share and the ownership share can be stacked to reveal the secret image for ownership identification. In the proposed scheme, the secret image is embedded with no modification of the host image. Besides, it is not necessary to employ the original host image and the assistance of computers to extract the hidden secret image. According to the experimental results, their scheme achieves stronger robustness against several common attacks when compared with existing schemes.

Ching-Sheng Hsu and Young-Chang Hou [69] proposed a novel copyright protection scheme for digital images based on visual cryptography (VC) and statistics. Owing to the fact that the parameters of the statistics of an image cannot be easily changed by many common attacks, sampling distribution of means (SDM) was employed to fulfill the requirements of robustness and comprehensibility. The host image is left unchanged by the proposed scheme which does not require the original image to identify the ownership. Therefore, the digital images that cannot be altered, such as, medical images are awfully appropriate for this scheme. Their method can recover the secret image with human eyes without the aid of computers, which completely utilizes the advantages of VC. The two-out-of-two VC scheme ensures the security, in which the SDM is used to assure the necessary probability setting. Hence, no one can recover any meaningful image or obtain any secret information without the correct private key. Consequently, wrapping of the transmission of secret images can be performed by this scheme. Even though, the method presently deals with only with bi-level secret images, the extension of the method to gray-level or color secret images will be concentrated in future.

5.2.2. Frequency Domain Methods

A wavelet-based watermarking technique that quantizes the so-called super trees for copyright protection was proposed by Shih-Hao Wang and Yuan-Pei Lin [70]. Every watermark bit is embedded in various frequency bands. The large spatial regions are spread throughout with the information of the watermark bit. The watermarking technique is vigorous to attacks in both frequency and time domains owing to the above feature. The robustness to frequency based attacks, for instance the removal of the high-pass band in low-pass processing, and the removal of high-pass details in JPEG compression was verified through the results in their paper. In addition, the robustness to time domain attacks such as pixel shifting and rotation was illustrated. Their proposed watermarking scheme supports data hiding or image authentication in addition to copyright protection.

Ying Yang et al. presented a removable visible watermarking scheme for combating copyright piracy, which operates in the discrete cosine transform (DCT) domain [71]. Firstly, the original watermark image is divided into 16×16 blocks and the element-by-element matrix multiplication on the DCT coefficient matrix of each block and a key-based matrix is performed to generate the preprocessed watermark to be embedded. This ensures that the unauthorized users cannot illegally remove the embedded watermark. Subsequently, to obtain a better match with the human visual system characteristics, the adaptive scaling and embedding factors for each block of the host image and the preprocessed watermark are calculated in accordance with the features of the corresponding blocks. In conclusion, the watermarked image is generated by adaptive addition of the significant DCT coefficients of the preprocessed watermark and the corresponding host image. The watermarking system is somewhat robust against compression. They verified the performance of their proposed method and the success of the introduced scheme in preventing the embedded watermark from illegal removal was illustrated through the results.

A semi-fragile watermarking technology was presented by Huang Ji-feng for copyright protection and image authentication [72]. In his method, the image is transformed into wavelet domain and the four adjacent wavelet coefficients are grouped. Owing to the fact that the mean has better stability than single wavelet coefficient, he embedded a digital signal into the average of the four adjacent wavelet coefficients using the characteristics of the human visual system. In, this method, the original image is not necessary when the watermark is extracted. The effectiveness of this method which is robust to common image process and fragile to malicious attack is illustrated through the results.

In fact conventional copyright protection mechanisms are not robust enough or embed the watermark into the host image using complex computations. An adaptive copyright protection scheme without the use of discrete cosine transformation (DCT) and discrete wavelet transformation (DWT) was proposed by Chin-Chen Chang and Pei-Yu Lin [73]. Their new approach improves the robustness of the watermark as it permits image owners to adjust the strength of watermarks through a threshold. Besides, diverse signal processing operations (such as blurring, JPEG compression, and noising) and geometric transformations (such as cropping, rotation, and scaling) are handled by their scheme. They illustrated that their scheme is superior to related works in most cases through the results. In particular, their scheme is appropriate for medical and artistic images as it maintains the data lossless requirement.

A novel algorithm based on Harr discrete wavelet transform for the grayscale watermark was presented by Ester Yen and Kai-Shiang Tsai [74]. Digital watermark for copyright protection of electronic documents and media is an extremely accepted research. The information hidden in electronic media is increasing owing to the rapid advancement in information technology. A visual cryptographic approach for producing two random shares of a watermark: one embedded into the cover-image, another one kept as a secret key for the watermark extraction later, was proposed by the authors. This procedure would be dealt with Harr discrete wavelet transform and be left primary features of two shares. Their approach is specifically designed and cannot be changed or removed effortlessly. Their method can extract cognoscible graphic even after several attacks.

A digital watermarking algorithm for copyright protection that works on basis of the concept of embed digital watermark and modifying frequency coefficients in discrete wavelet transform (DWT) domain was presented by Abou Ella Hassanien [75]. He embeds the watermark into the detail wavelet coefficients of the original image through the aid of a key. This key produced at random and is employed to chose the precise locations in the wavelet domain where in the watermark needs to be embedded. The analogous watermark detection algorithm is offered. A novel metric that measures the objective quality of the image on basis of the detected watermark bit is brought in, which the original unmarked image is not necessary for watermark extraction. The performance of his proposed watermarking algorithm is robust to a broad range of signal distortions including JPEG, image cropping, geometric transformations and noises.

Reddy and Chatterji [76] presented a new wavelet based logo-watermarking scheme for copyright protection of digital image. Watermark employed is a visually meaningful gray scale logo rather than a noise type Gaussian sequence. Both the image and logo are transformed in wavelet domain to embed the watermark. The significant coefficients of each sub-band selected by considering the human visual system (HVS) characteristics are added with the watermark bits, thus, the embedded watermark is robust and imperceptible. A scheme that intends to extract watermark from distorted images in a reliable manner is devised. The robustness of their proposed method against a variety of attacks is illustrated through the experimental results. The superiority of their method was illustrated by its comparison with the existing methods.

5.2.3. Other Researches

The abundance of digitized images had necessitated the urgent requirement for copyright enforcement schemes that aid in the protection of copyright ownership. The watermarking system is considered as an exceptional method to guard copyright ownership [77]. Ren-Junn Hwang [78] proposed a watermark method that works on basis of visual cryptography. According to their proposed method, the watermark pattern need not necessarily be embedded into the original image directly, which makes it tedious to identify or recover it from the marked image in an illegal manner. It is possible to retrieve it devoid of making any comparison with the original image. Further, the notary can as well off-line adjudge the ownership of the suspect image by their method. The watermark pattern can be some noteworthy black/white image that can be employed to personify the owner. Results illustrate that the watermark pattern in the marked image has superior transparency and robustness.

A digital image copyright protection method which does not require the watermark pattern to be embedded in to the original image which leaves the marked image equal to the original image was presented by Azzam SLEIT and Adel ABUSITTA [79]. Intended for rotated and resized images or group of images, the watermark pattern is retrieved in its present condition. In comparison to other techniques, the proposed technique protects a group of images demonstrating its dominance. The key is necessary to retrieve the watermark pattern from the marked image. Moreover, even when all the algorithm components are known, it is not possible to retrieve the key. The length of the given key controls the security of the method. The security of method is less for shorter keys, whereas the security is higher in the case of very long keys.

The scheme that attempts to solve the ownership problem was presented by Qiao et al. [81]. They generated the randomized watermarks from the original image or video chip by combining their scheme with cryptography and utilizing a standard encryption algorithm (i.e. DES). The function of the encryption key and the original image is the embedded watermark. The inability of the algorithm to insert semantically meaningful watermarks and the critically restricted capacity of watermarks are the evident drawbacks of their scheme. Additionally, it is complicated to estimate the inserted watermark's energy and capacity and to control the visual quality of the watermarked images as it is a non-linear watermarking model.

Some scenarios in which many current watermarking schemes fail to resolve the rightful ownership of an image has been discussed by Zeng et al. [80]. Essentially, their watermarking scheme cannot resolve rightful ownership as the embedded watermark is detected without using the original image [81]. Instead of protecting the ownership of digital images, the watermarking scheme in their algorithm protects the embedded watermark. Owing to the fact that watermark detection in their algorithm does not require original images, an attacker can always create his counterfeit original images and claim his/her ownership, this is a key problem.

A novel digital watermarking technique which promises both Security and Quality for the image for the Patent protection was presented by Yamuna Govindarajan and Sivakumar Dakshinamurthi [82]. The scores of issues addressed in data encryption and watermarking in a DRM, given the drive toward security for emerging resource constrained DRM applications has been outlined. Moreover, a new architecture for Patent Protection that holds pledge for a better compromise between practicality and security for emerging digital rights management application was proposed by the authors. The authors proposed the five level securities which can secure the data from hacking in this present solution. Hence, a prototype shift in the area of information protection, in which ideas from areas for instance media processing are often incorporated to provide more lightweight solutions is created.

The importance of the integrity protection of XML documents is increasing owing to the fast development of Extensible Markup Language (XML) and its comprehensive application. A XML watermarking scheme that employs the convolution operation to provide a solution to the integrity protection of XML documents was presented by Ronghua Yao et al. [30]. It is the most time-consuming part of their whole algorithm although it can diffuse and amplify possible modifications. Moreover, to promote the framework further to real applications, the security of their proposed watermarking scheme is theoretically analyzed. They illustrated that the XML watermarking scheme is a promising tool for the integrity protection of XML documents through the extensive experiments conducted that conclude that: (a) their proposed watermarking scheme efficiently protects the integrity of XML documents, (b) in comparison to the signature methods which attach the additive signatures to the original documents thus, expanding their size, the presented watermarking scheme does not increase the file size of XML documents, (c) in addition, the traditional signature methods are outperformed by the proposed XML watermarking scheme in combination with PCA and ULC in terms of time spent by the algorithms.

The main facet for highly dynamic group communication where the members can join or leave the group at their will is the security in dynamicity. In addition, there is an increased pursuit for copyright protection of their fruitful work. The issues of scalability of the groups and ownership rights of the contents are left unaddressed by the existing architectures. A secure, efficient and scalable multicast architecture that employs the same tree structure to ensure confidentiality and also to provide ownership rights was presented by Vijayaraghavan and Wahida Banu [36]. The remarkable changes necessary in multicast key management architecture is observed in this work. An attempt to evade the unauthorized duplication of data is also made in this work.

6. Conclusion

Digital Watermarking is a novel and budding research field. It chiefly includes the addition of hidden messages or copyright notices in digital media. Each and every watermarking system is devised to attain one goal which is embedding a hidden robust watermark into digital media. These systems are bound to satisfy two conflicting requirements. First, the watermark needs to be resistant against intentional and unintentional removal. Then, watermarked image needs to sustain a good fidelity i.e. watermark needs to be perceptually undetectable. In order to achieve this task, a wide range of techniques have been exploited, and diverse domains are included so as to improve a certain application of watermarking and/or enhance fidelity and robustness of watermarked signal. In this paper, we have presented a comprehensive survey of the significant techniques in existence for watermarking those are employed in copyright protection. Along with this, an introduction to digital watermarking, properties of watermarking and its applications have been presented. The aim of this research is to assist the budding researchers in the field of digital image watermarking for copyright protection to understand the available methods and to aid their research further.

References

[1] A. Piva, F. Bartolini, and M. Barni, “Managing copyright in open networks,” IEEE Transactions on Internet Computing, Vol. 6, No. 3, pp. 18–26, May–June 2002.

[2] C. Lu, H. Yuan, and M. Liao, “Multipurpose watermarking for image authentication and protection,” IEEE Transactions on Image Processing, Vol. 10, No.10, pp. 1579–1592, October 2001.

[3] Tosihiro Akiyama, Fumiaki Motoyoshi, Osamu Uchida and Shohachiro Nakanishi "Hybrid Digital Watermarking for Color Images Based on Wavelet Transform," IADIS International Conference Applied Computing 2006, San Sebastian, Spain, February 2006.

[4] Memon, N. and Wong, P., “Protecting Digital Media Content,” In: Communications of ACM, Vol. 41, No. 7, pp. 35-43, July 1998

[5] G. Voyatzis and I. Pitas, “The use of watermarks in the protection of digital multimedia products," IEEE Proceedings, Vol. 87, No. 7, pp 1197-1207, July 1999.

[6] Authors Emir Ganic, Ahmet M. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies", International Multimedia Conference, Magdeburg, Germany, pp. 166 - 174, 2004.

[7] Xiang-Yang Wang and Hong Zhao, "A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT", IEEE Transactions On Signal Processing, Vol. 54, No. 12, December 2006.

[8] Miller, M.; Cox, I.J.; Linnartz, J.P.M.G.; Kalker, T., “A review of watermarking principles and practices,” In Digital Signal Processing in Multimedia Systems, Edit. K. K. Parhi and T. Nishitani, Marcell Dekker Inc., pp. 461-485, 1999.

[9] Xiaoqiang Li, Xiangyang Xue and Wei Li, "An Optimized Multi-bits Blind Watermarking Scheme," Lecture Notes in Computer Science, Vol. 2836, pp.360-369 , 2003.

[10] P. Tao and A. M. Eskicioglu, “A Robust Multiple Watermarking Scheme in the DWT Domain,” Optics East 2004 Symposium, Internet Multimedia Management Systems V Conference, Philadelphia, PA, pp. 133-144, October 25-28, 2004.

[11] Ersin Elbasi and Ahmet M. Eskicioglu, “A Semi-Blind Watermarking Scheme for Color Images Using a Tree Structure," in proc. of IEEE Sarnoff Symposium, March, 2006.

[12] Yeung, M. & Minzter, F., “An Invisible Watermarking technique for image verification,” Proceeding on the IEEE International Conference on Image Processing, pp: 680-683, 1997.

[13] Shaowei Weng, Yao Zhao and Jeng-Shyang Pan, “A Novel Reversible Data Hiding Scheme,” International Journal of Innovative Computing, Information and Control, Vol. 4, No. 2, pp. 351-358, 2008.

[14] G. Coatrieux, H. Maître, B. Sankur, Y. Rolland, R. Collorec, "Relevance of Watermarking in Medical Imaging," in Proc. IEEE Int. Conf. ITAB, USA, pp. 250–255, 2000.

[15] Cox I. J., Miller, M. L. and Bloom J. A., “Digital Watermarking”, Morgan Kaufmann Publishers, USA, 2002.

[16] Katzenbeisser S. and Petitcolas F. A. P., “Information Hiding Techniques for Steganography and Digital Watermarking”, Artech House, UK, 2000.

[17] Craver, S.; Memon, N.; Yeo, B.-L.; Yeung, M.M.; “Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications,” IEEE Journal on Selected Areas in Communications, Volume: 16, Issue: 4, Pages: 573 -586, May 1998.

[18] Craver, S.; Memon, N.; Boon-Lock Yeo; Yeung, M.M.; “On the invertibility of invisible watermarking techniques,” Proceedings of International Conference on Image Processing, Volume: 1, Pages: 540 -543, Oct. 1997

[19] Craver, S.A.; Min Wu; Liu, B.; “What can we reasonably expect from watermarks?,” IEEE Workshop on the Applications of Signal Processing to Audio and Acoustics, Pages: 223 -226, Oct. 2001.

[20] G. W. Braudaway abd K. A. Magerlein and F. C. Mintzer, “Color correct digital watermarking of images,” Technical Report 5,530,759, United States Patent, 1996.

[21] Md. Mahfuzur Rahman and Koichi Harada, "Parity enhanced topology based spot area watermarking method for copyright protection of layered 3D triangular mesh data", IJCSNS International Journal of Computer Science and Network Security, Vol.6, No.2A, February 2006.

[22] M. Hamad Hassan, and S.A.M. Gilani, "A Fragile Watermarking Scheme for Color Image Authentication", International Journal of Applied Science, Engineering and Technology, Vol. 1, No. 3, pp.156-160, 2005.

[23] Francesco Benedetto, Gaetano Giunta, Alessandro Neri, “A New Color Space Domain for Digital Watermarking in Multimedia Applications”, IEEE International Conference on Image Processing, ICIP 2005, Vol. 1, pp. I- 249-52, 11-14 September 2005.

[24] G. Voyatzis, I. Pitas, “Applications of Toral Automorphism in Image Watermarking,” ICIP 1996, Vol. II, pp.237-240, 1996.

[25] Xiangui Kang, Jiwu Huang, and Wenjun Zeng, "Improving Robustness of Quantization-Based Image Watermarking via Adaptive Receiver", IEEE Transactions on Multimedia, Vol. 10, No. 6, pp. 953-959, October 2008.

[26] J. Huang, Y. Q. Shi, “Reliable information bit hiding,” IEEE Transactions on Circuits and Systems for Video Technology, Vol.12, No.10, pp. 916~920, 2002.

[27] D. Kundur and D. Hatzinakos, "Diversity and attack characterization for improved robust watermarking," IEEE Transactions on Signal Processing, Vol. 49, No. 10, pp. 2383-2396, 2001.

[28] X. Kang, J. Huang, and Y. Q. Shi, Y. Lin, “A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression,” IEEE Transactions on Circuits and Systems for Video Technology, Vol.13, No. 8, pp.776-786, August 2003.

[29] C.S. Lu, S.K. Huang, C.J. Sze, and H.Y. Liao, "Cocktail watermarking for digital image protection," IEEE Transactions on Multimedia, Vol.2, No.4, pp.209–224, December 2000.

[30] Ronghua Yao, Qijun Zhao, and Hongtao Lu, "A Novel Watermark Algorithm for Integrity Protection of XML Documents", IJCSNS International Journal of Computer Science and Network Security, Vol.6 No.2B, pp. 202-207, February 2006.

[31] T. Furon and F. P. Duhamel, “Robustness of an asymmetric watermarking method,” in Proc. IEEE Int. Conf. on Image Processing, Vancouver, Canada, vol. III, pp. 21–24, 2000.

[32] D. Kundur, “Energy allocation for high-capacity watermarking in the presence of compression,” in Proc. IEEE Int. Conf. Image Processing, Vancouver, BC, Canada, Vol. I, pp. 423–426, 2000.

[33] C. S. Lu, H. Y. Mark Liao, and L. H. Chen, “Multipurpose audio watermarking,” in Proc. 15th Int. Conf. on Pattern Recognition, Barcelona, Spain, vol. III, pp. 286–289, 2000.

[34] C. S. Lu and H. Y. Mark Liao, “Oblivious cocktail watermarking by sparse code shrinkage: A regional- and global-based scheme,” in Proc. IEEE Int. Conf. on Image Processing: Special Session on Second Generation Watermarking Methods, Vancouver, BC, Canada, vol. III, pp. 13–16, 2000.

[35] S. D. Servetto, C. I. Podilchuk, and K. Ramchandran, “Capacity issues in digital image watermarking,” presented at the 5th IEEE Conf. Image Processing, 1998.

[36] V. Vijayaraghavan, R.S.D. Wahida Banu, "Efficient Key Management Architecture with Copyright Protection for Dynamic Groups", Journal of Theoretical and Applied Information Technology, Vol.3, No. 2, pp. 60-64, 2007.

[37] M. L. Miller, G. J. Doerr and I. J. Cox, "Applying Informed Coding and Embedding to Design a Robust, High capacity Watermark", IEEE Transactions on Image Processing, Vol. 13, No. 6, pp. 792-807, June 2004

[38] Zhe-Ming Lu, Wei-Min Zheng, Jeng-Shyang Pan and Zhen Sun, "Multipurpose Image Watermarking Method Based on Mean-removed Vector Quantization", Journal of Information Assurance and Security, Vol. 1, pp. 33-42, 2006.

[39] H. C. Huang, F. H. Wang and J. S. Pan, “A VQ-based Robust Multi-watermarking Algorithm”, IEICE Transactions on Fundamentals, Vol. E85-A, No. 7, pp. 1719-1726, 2002.

[40] Ruizhen Liu; Tieniu Tan, "An SVD-based watermarking scheme for protecting rightful ownership", IEEE Transactions on Multimedia, Vol. 4, No. 1, pp. 121-128, March 2002.

[41] Wei Lu, Hongtao Lu, "Robust Watermarking based on Sub-sampling and Nonnegative Matrix Factorization", Informatica, Vol. 19, No. 4, pp. 555-566, December 2008.

[42] Chin-Chen Chang , Hsien-Wen Tseng, “VQ-Based Image Watermarking Using Anti-Gray Coding”, Informatica, v.15 n.2, p.147-160, April 2004.

[43] C. Lin, M. Wu, Y. M. Lui, J. A. Bloom, M. L. Miller, I. J. Cox, "Rotation, Scale, and Translation Resilient Public Watermarking for Images", IEEE Transactions on Image Processing, Vol. 10, No. 5, pp. 767-782, 2001.

[44] R. N. Bracewell, "The Fourier Transform and Its Applications," New York: McGraw-Hill, 1986.

[45] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science, Vol. 3, No.9, pp. 740-746, 2007

[46] Muhammad Shafique Shaikh and Yasuhiko Dote, "A Watermarking Scheme For Digital Images Using Multilevel Wavelet Decomposition", Malaysian Journal of Computer Science, Vol. 16 No. 1, pp. 24-36, June 2003.

[47] Jung-Chun Liu, Chu-Hsing Lin, Li-Ching Kuo and Jen-Chieh Chang, "Robust Multi-scale Full-Band Image Watermarking for Copyright Protection", Lecture Notes in Computer Science, Springer Berlin, Heidelberg, Vol. 4570, pp. 176-184, 2007.

[48] Yen-Chung Chiu and Wen-Hsiang Tsai, "Copyright Protection against Print-and-Scan Operations by Watermarking for Color Images Using Coding and Synchronization of Peak Locations in Frequency Domain", Journal Of Information Science And Engineering, Vol. 22, pp. 483-496, 2006.

[49] Y. Yang, X. Sun, H. Yang, and C.T. Li, "A Removable Visible Image Watermarking Algorithm in DCT Domain," Journal of Electronic Imaging, Vol. 17, No. 3, pp. 033008-1 ~ 033008-11, July - September, 2008.

[50] Azadeh Mansouri, Ahmad Mahmoudi Aznaveh and Farah Torkamani Azar, "Secure Digital Image Watermarking Based on SVD-DCT", Communications in Computer and Information Science, Springer Berlin Heidelberg, Vol. 6, pp. 645-652, 2008.

[51] Fangjun Huang, Zhi-Hong Guan, "A hybrid SVD-DCT watermarking method based on LPSNR", Pattern Recognition Letters, Vol. 25, No. 15, pp. 1769-1775, November 2004.

[52] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Transactions on Image Processing, Vol. 6, pp. 1673–1687, January 1997.

[53] W. Zhu, Z. Xiong, and Y.Q. Zhang, “Multiresolution watermarking for images and video,” IEEE Transactions on Circuits and Systems for Video Technology, Vol. 9, pp.545–550, June 1999.

[54] G. C. Langelaar and R. L. Langendijk, “Optimal differential energy watermarking of DCT encoded images and video,” IEEE Transactions on Image Processing, Vol. 10, pp. 148–158, Jan. 2001.

[55] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Attacks on copyright marking systems,” in Proc. 2nd Workshop on Information Hiding, Lecture Notes in Computer Science, Vol. 1525, April 1998 .

[56] Wu, C. and W. Hsieh, "Digital watermarking using zerotree of DCT," IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, pp: 87-94, 2000.

[57] Chang-Hsing Lee, Yeuan-Kuen Lee, "An adaptive digital image watermarking technique for copyright protection",

IEEE Transactions on Consumer Electronics, Vol. 45, No. 4, pp. 1005 - 1015, November 1999.

[58] Andrew B. Kahng, John Lach, William. H. Mangione-Smith, Stefanus Mantik, Igor L. Markov, Miodrag Potkonjak, Paul Tucker, Huijuan Wang, and Gregory Wolfe, "Constraint-Based Watermarking Techniques for Design IP Protection", IEEE Transactions On Computer-Aided Design Of Integrated Circuits And Systems, Vol. 20, No. 10, October 2001.

[59] T. Furon and P. Duhamel, "An Asymmetric Watermarking Method", IEEE Transaction on Signal Processing, Vol. 51, No. 4, pp. 981- 995, April 2003.

[60] T. Kalker, "A security risk for publicly available watermark detectors," in proceedings Benelux Information Theory Symposium, Veldhoven, The Netherlands, May 1998.

[61] Xu Zhou, Yu Ren, and Xuezeng Pan, "Watermark Embedded in Polygonal Line for Copyright Protection of Contour Map", IJCSNS International Journal of Computer Science and Network Security, Vol.6 No.7B, pp. 202-205, July 2006.

[62] Jengnan Tzeng, Wen-Liang Hwang, and I-Liang Chern, "An Asymmetric Subspace Watermarking Method for Copyright Protection", IEEE Transactions on Signal Processing, Vol. 53, No. 2, February 2005.

[63] Yamuna Govindarajan, Sivakumar Dakshinamurthi "Copyright protection protocols for copyright protection issues", WSEAS Transactions on Computer Research, Vol. 3, No. 4, pp. 242-251, April 2008

[64] Min-Jen TSAI and Chang-Hsing SHEN, "Differential Energy Based Watermarking Algorithm Using Wavelet Tree Group Modulation (WTGM) and Human Visual System", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E91-A, No. 8, pp. 1961-1973, 2008.

[65] Ming-Chiang Hu, Der-Chyuan Lou and Ming-Chang Chang, "Dual-wrapped digital watermarking scheme for image copyright protection," Computers & Security, Vol. 26, No. 4, pp. 319-330,2007.

[66] Hernandez, J.R., Perez-Gonzalez, F., "Statistical analysis of watermarking schemes for copyright protection of images", Proceedings of the IEEE, Vol. 87, No. 7, pp. 1142 - 1166, July 1999.

[67] Rawan I. Zaghloul, Enas F. Al-Rawashdeh, "HSV Image Watermarking Scheme Based on Visual Cryptography", Proceedings of World Academy of Science, Engineering and Technology Vol. 34, October 2008.

[68] Ming-Shi Wang and Wei-Che Chen, "Digital image copyright protection scheme based on visual cryptography and singular value decomposition", Optical Engineering, Vol. 46, No. 6, 2007.

[69] Ching-Sheng Hsu, Young-Chang Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods", Optical Engineering, Vol. 44, No. 7, July 2005.

[70] Shih-Hao Wang and Yuan-Pei Lin, "Wavelet Tree Quantization for Copyright Protection Watermarking", IEEE Transactions On Image Processing, Vol. 13, No. 2, February 2004.

[71] Ying Yang, Xingming Sun, Hengfu Yang, Chang-Tsun Li, "Removable visible image watermarking algorithm in the discrete cosine transform domain", Journal of Electronic Imaging, Vol. 17, No. 3, 2008.

[72] Huang Ji-feng, "Semi-fragile watermarking for copyright protection and image authentication," Wuhan University Journal of Natural Sciences, Vol. 1, No. 1, pp. 284-288, 2005.

[73] Chin-Chen Chang, Pei-Yu Lin, "Adaptive watermark mechanism for rightful ownership protection," Journal of Systems and Software, Vol. 81, No. 7, pp. 1118-1129, 2008.

[74] Ester Yen, Kai-Shiang Tsai, "HDWT-based grayscale watermark for copyright protection," An International Journal Source Expert Systems with Applications, Vol. 35, No. 1-2, pp. 301-306, 2008.

[75] Abou Ella Hassanien, "A Copyright Protection using Watermarking Algorithm", Informatica, Vol. 17, No. 2, pp. 187-198, April 2006.

[76] Reddy, A. and B. Chatterji, "A New Wavelet Based Logo-watermarking Scheme," Pattern Recognition Letters, Vol. 26, No. 7, pp. 1019-1027, 2005.

[77] Hwang M. S., Chang C. C., and Hwang K. F., "A Watermarking Technique Based on One-way Hash Functions," IEEE Transactions on Consumer Electronics, Vol. 45, No. 2, pp. 286-294, 1999.

[78] Ren-Junn Hwang, "A Digital Image Copyright Protection Scheme Based on Visual Cryptography", Tamkang Journal of Science and Engineering, Vol. 3, No. 2, pp. 97-106, 2000.

[79] Azzam SLEIT, Adel ABUSITTA, "A Visual Cryptography Based Watermark Technology for Individual and Group Images", Journal of Systemics, Cybernetics and Informatics, Vol. 5, No. 2, pp. 24-32, 2008

[80] W. Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images", IEEE Transactions on Image Processing, Vol. 8, No. 11, pp. 1534-1548, 1999.

[81] L. T. Qiao and K. Nahrstedt, "Watermarking schemes and protocols for protecting rightful ownership and customer's rights", Journal of Visual Communication and Image Representation, Vol.9, No.3, pp.194-210, 1998.

[82] Yamuna Govindarajan, Sivakumar Dakshinamurthi, "Quality - Security uncompromised and Plausible Watermarking for Patent Infringement", International Journal of Image Processing, Vol. 1, No. 2, pp. 11-20, July/August 2007.

[83] "Digimarc Corporation" from https://digimarc.com/appdev/.

Mr.Manjunatha Prasad.R is currently working as a Assistant Professor in the department of Electronics at K.S.Institute of Technology, Bangalore. He obtained his B.E. degree in E & C during 1993 from Bangalore University & M.E. degree in Digital Electronics in 1998 from Karnatak University, Dharwad. He has one international conference & two national conference publications. Presently, he is pursuing his Ph.D at Malnad College of Engineering, Hassan under VTU. His areas of interest are Digital Image Processing & Digital System Design.

Dr.Shivaprakash Koliwad is currently working as a Professor& Head in the department of Electronics at Malnad College of Engineering, Hassan. He obtained his B.E degree in E & C during 1976 from SJCE, Mysore University, M.Tech during 1994 from IIT, Delhi & Ph.D during 2000 from Anna university. He has authored many publications & books. His areas of interest are Multi-rate signal processing, Bio-medical, Digital image processing & Multimedia.