Digital Watermarking Properties, Classification and Techniques

A. Al. Embaby, Mohamed A. Wahby Shalaby, Khaled Mostafa Elsayed

Abstract: *The rise in the demand for multimedia digital products has led to significant copyright challenges, which concerns proof of ownership and copy control. Digital watermarking method provides a solution to the problems associated to copyright protection and control. Considerable quantities of multimedia content are printed, edited or distributed unlawfully without the legal consent of the owner. Digital piracy in the movie and music industry contributes to severe economic losses annually. The problem of digital piracy has led to the urgent need for digital watermarking as a method to counter the piracy. The protection of digital content is currently the main responsibility of the content owner since piracy is evident in all levels of multimedia industry. Therefore, for multimedia information, protection of content copyright has increasingly become the sole focus of the content owner. Digital watermarking is a vital technology, which is applicable in protecting the contemporary multimedia digital contents..*

Keywords: copyright protection, digital watermarking, visible watermar,.

I. INTRODUCTION

With the discovery of the numeric period towards the end of the 20th century, transfer of digital data became more possible and easier. This revolutionary technology, which saw the swift migration from analog to digital technology generated a lot of anxiety regarding the protection of copyrights because multimedia digital information is easily accessible and transferable. People can easily edit, duplicate and unlawfully transfer digital content without the approval of the content owner. Digital content owners are driven to ensure the safety of their multimedia content. The conventional technology for copyright protection is cryptography, which uses a secret key in order to secure the digital content and generate a ciphered content. However, when the cipher content is cracked, the hacker can easily access the protected documents. This leads to the insecurity of the intellectual property. The owner of the content is thus, not in a position to determine the documents accessed illegally leading to economic losses. These uncertainties led to the discovery of a more complex technology that can ensure the security of multimedia digital content.

Information encrypting technology hides vital data in other open digital products. The technology then transfers vital data through the delivery of open carriers leading to creation of effective means for the realization of secure transfer of confidential data within the network [1]. The information hiding system is described in Figure 1 below.

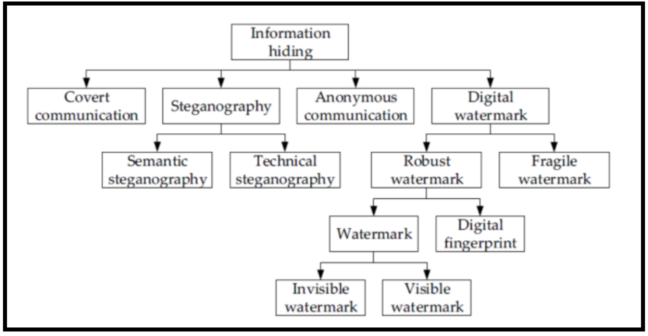

Fig. 1 Branches of information hiding, Figure taken from [1]

Between the systems of information hiding, the digital watermark can genuinely remedy the shortcomings experienced in the protection of digital content. Digital watermarking concerns marking of digital data known as watermark, into a multimedia digital content normally referred to as host signal or original content. The embedment is performed in a manner that ensures the detection or extraction of the watermark later without destroying the host signal. Normally, malicious infections try to penetrate the watermark protection by configuring the technology's weak points. Therefore, it is important to perform frequent maintenance and system updates for the watermarking technology to enhance the security of the technology.

Due to the growth and publication of the internet and the increase in several broadcast avenues, digital movies and videos have found their ways to all spheres of life. Accordingly, all types of illegal videos and printed contents are all over the internet. This violates the copyrights of the original content owners, and hinders the growth of multimedia digital industry. Thus, severe video watermarking technology for protecting digital video information has been developed to help curb the problem.

Revised Manuscript Received on February 15, 2020.
* Correspondence Author

A. Al. Embaby *, Department of Information Technology, Faculty of Computers and Artificial Intelligence, Cairo University, Giza – Egypt : Email: embaby.ahmed@gmail.com

Mohamed A. Wahby Shalaby, Department of Information Technology, Faculty of Computers and Artificial Intelligence, Cairo University, Giza – Egypt: Email:: m.wahby@fci-cu.edu.eg

Khaled Mostafa Elsayed, Department of Information Technology Department, Faculty of Computers and Artificial Intelligence, Cairo University, Giza – Egypt: Email: khaledms@gmail.com

There are various types of watermarking but visible watermarking technology provides a more active protection of digital content since it not only avoids pirates from hacking the digital information, but also recognizes the security of multimedia information visually. Digital information protected by visual watermark provides recognizable, but unbreakable copyright system, which discovers the content owner. A visible watermarking technology should contain information of the content that can ensure that the security patterns are difficult to configure making it impossible for unauthorized persons to access the watermarked data.

This study paper gives a general view of the digital watermarking technology. This study paper takes the following organization; section 2 provides an overview of digital watermarking, Properties, classification, and types. In section 3, an overview of different watermarking approaches. Video watermarking is discussed in section 4, and quality assessment of visible watermarking is introduced in section 5. Section 6 is the last section and provides conclusion and recommendations for future studies.

II. WATERMARKING

The past few years have seen robust use of the internet enabled by the tremendous technological advancements in the multimedia industry. The internet usage has extremely attained heights in multimedia technology. Since the growth of the internet usage, digital multimedia data have remained under great threat of hacking and unauthorized access. Larger amounts of multimedia information are distributed, edited and printed without the consent of the author [2]. The unauthorized access of the digital intellectual property leads to severe economic losses in the movie and music industry annually. This has led to the urgent and increasing need for digital watermarking technology to help in solving the piracy problems. Thus, the protection of the digital intellectual property has become the main aim of the content owners. Digital watermarking technology has emerged as the most efficient method of protecting digital content against unauthorized access. The field of digital multimedia witnesses a lot of research directed towards effective mechanisms of applying digital watermarking technology in the protection of the digital content [3].

Watermark is a kind of text that is inserted in an image or video to provide verification and confirmation of the image or the video's authority. Watermarking is considered as a protection method for the digitalized information in the current world. Recently, the digital market has witnessed extensive usage of the internet to request methods to protect the copyright of digital content. Digital watermarking technology provides reliable solution to the disturbing problems of pirating digital content [4].

Digital watermarking includes the embedding of a data that represent the copyright or authentication, this data referred to as watermark, through a series of objects (host signal or original content) in a manner that watermark may be discovered or withdrawn later when necessary without destroying the host signal [5,6]. Digital watermark technology broken down contains a detector and an embedded. The embedded contains the watermark information. The extractor is designed to establish the presence of a watermark in the digital data [7]. A simplified watermarking system is described in Figure 2.

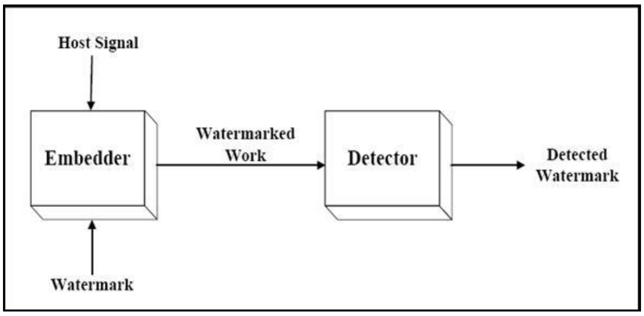

Fig. 2 A simple digital watermarking scheme.

A. Watermarking Properties

Many defining properties can describe a watermarking system, while the system will control, which properties should be confirmed [8]. Hereafter we will highlight the main properties of watermarking schemes [9].

- **Robustness**: This property enables the technology to notice or recognize the embedded watermark after a given signal analysis undertaking [10, 11]. In the same time, the watermark should also be able to survive against malicious attacks, but digital watermark cannot survive against all types of attacks. So, the attacks techniques should be optimized based on the application. As an example, when authenticating digital images, we are checking the data integrity in order to detect any manipulations [11].The strong video watermark is a critical stratum of the digital video watermark, which applies provisional redundancy and partially segmented redundancy of the contents of a video to install watermark for the copyright protection of the video. General strong video watermark is an essential digital video watermarks branch using video content temporal and spatial redundancy in embedding watermark information to achieve the protection of a video copyright. General robust video watermarking schemes include three components: watermark detection, also known as extraction, generation and embedding. The algorithm emphasis in these three parts will also change accordingly from the point of view of the application of watermark technology.
- **Fidelity**: In this context, the fidelity of a watermarking system refers to the similarity of perception between the watermarked and un-watermarked works at the point of their presentation to the consumer [9]. This characteristic also refers to invisibility and preserves the resemblance between the original image and the watermarked object in view of the human perception [10]. The mark must remain invisible in invisible watermark in spite of the little degradations in the brightness or contrast of the image.
- **Security**: Unauthorized users are not in a position to detect and neither can they retrieve, or change the embedded watermark.

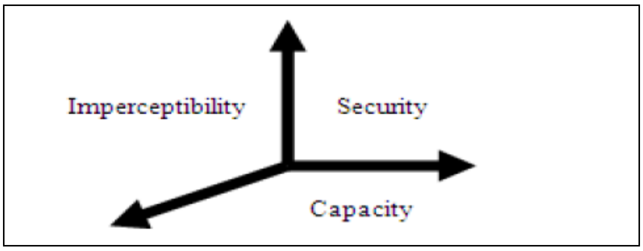

Fig. 3 Characteristics of digital watermarking

- **Transparency**: Transparent watermark should not cause any structure or feature loss on the original digital content. Also, no artifacts on the original content is allowed.
- **Capacity**: watermarking capacity is the information quantity that the host data can embed. The volume of data that can be embedded using watermarking system depends on the use. A mark will always be a static set of bits in the case of images. The capacity in videos will always be assessed by the number of bits per frame inserted but the number of bits per second in audio files [10]. The requirement in capacity is always the effort gauged against two other essential requirements that include robustness and imperceptibility (Figure 3). Usually, to achieve greater capacity it will be in the expense of the imperceptibility or robustness level of strength or both.
- **Detection Types**: this property defines which resources are necessary for the extraction of the embedded watermark into the watermarked information

B. Classification

The classification of a watermarking system occurs on the basis of requirements as follow:

- **Robustness based classification**: based on robustness classification takes place in terms of the following:

a) **Fragile**: the destruction of the watermark can be because of small manipulations of the image watermarked [12]. This type of watermark can be applicable in the authentication and verification of integrity.

b) **Semi Fragile**: they act like fragile watermarks in the face of intended changes but as robust watermarks against common alterations [13] such as noises. They have been applied in the authentication and taper control of images.

c) **Robust**: the design of these watermarks is to enable them to resist heterogeneous manipulations according to [12]. Their application is in copy control and e monitoring.

- **Detection Types based classification**:

a) **Blind**: Here, the receiver does not have access to the mark data and original image because it is not available. For example, the copy control applications must be in a position to transmit varying watermarks to every user while the receiver must be equipped to identify and interpret the various marks [10].

b) **Non-Blind**: Here, the receiver requires the original information or some data derived from it to help in the detection process [10]. The information will also help in the process of algorithm extraction.

The watermarking system also classified based on the embedding method. The technique of embedding used for the watermark affects the algorithm of detection as well as the strength during attacks. According to [14], the person responsible for the process of designing a watermark must evaluate the costs and benefits in the simple characteristics of fidelity, payload, and robustness. Based on the embedding process, we can have two different approaches:

a) **Spatial Domain**: For example, if the host content is an image, and we need to embed an invisible watermark, the spatial domain watermarking system inserts information into in the outer image, altering image characteristics or pixels [12]. These algorithms must weigh between amount of converted bits into pixels and the chances of the watermark being invisible [14]. These watermarking schemes are recommended for tamper detection and document authentication.

b) **Transform Domain**: The techniques embed watermarking data in transform coefficients of the digital content, subsequently scattering the data via the frequency spectrum [10]. This process makes it difficult to detect and strengthens alterations from alterations arising from the processing of signals. The most commonly used transforms include Discrete cosine transform (**DCT**) [10], discrete wavelet transform (**DWT**) [15] as well as discrete lifting transform (**LWT**) [16].

The classification of watermarking according to perceptivity occurs in two classes namely:

a) **Visible watermarking**: This refers to the process of embedding information into a multimedia such as a video or image to make it perceptible to a human observer.

b) **Invisible watermarking**: Invisible digital watermarking (IDW) is a special kind of steganography, at which hiding information in digital content to prove integrity, ownership, or provide additional information. In the case of copyright, robustness against destruction and spoofing will be its priority.

III. WATERMARKING TECHNIQUES

The Digital watermarking techniques are categorized in terms of the algorithm used on the method of embedding. The watermark embedding algorithm is a process to embed binary data into an original product to prove the ownership or copyright information. The embedding algorithm must take into account the balance between the invisibility of the watermark and its robustness. Generally, watermarking techniques is classified based on different embedding domain of the watermark into two classes, spatial and transform domain or the frequency domain. In the **video watermarking algorithm**, the techniques of watermarking can be classified into three forms depending on the embedding position of the watermark: video watermarking algorithm during the encoding process, original video-based watermarking algorithm, and video watermarking algorithm after compression.

A. Spatial Domain Watermarking Schemes

In this category of watermarking techniques, the embedment of the watermark occurs by modifying the raw content directly (i.e., the pixel values of the main image/video) of the original product.

In image and video watermarking, the most important advantages of spatial domain-based methods are its simplicity to be implemented with low computational complexities. These techniques, therefore, are used in video watermarking extensively, where performance in real time is the main concern [2]. The watermark that results from the process may or may not be noticeable, depending on the value of the intensity of the pixel. picture cropping, for example, is a common tool by image editors to remove the watermark [17]. Hereafter we will introduce main techniques of the spatial domain-based watermarking techniques:

1) **Correlation-based Techniques**: where the watermark **W(i, j)** is added directly to the original content **I(i, j)** in relation to (1).

$$I_w(i,j)=I(i,j)+\alpha W(i,j) \qquad (1)$$

Where **α** is a gain factor, **I_w** is the watermarked content, and **(i, j)** is the index of 2D data array. As the gain factor **α increase**, the watermark quality contents will be expensed.

2) **Least Significant Bit Modification (LSB):** LSB is the most straightforward method since the least essential bits contain the most irrelevant data as well as the alteration does not lead to perceptible changes. In the midst of these approaches, there are types that use only the mild points [18] as well as type that applies cryptography on the message in the watermark before the process of embedding [19], In the latter case, a key is used to create a cipher called "data mark" is and this is embedded in the cover image. This key helps in determining the points, which the embedding process must modify. In the process, the algorithm is an inverse to the embedding. It is essential to analyze the object and isolate its least significant bit. Together with the cryptography keys, the extracted bits help in decoding algorithms to recover the initial watermark. However, it is a widely used technique because of its simplicity but has certain shortcomings such as like poor quality of the produced video, inability to deal with a range of attacks, and a lack of imperceptibility and the least robustness [20].

3) **Singular Value Decomposition (SVD)**: SVD refers to linear algebra numerical analysis used in many applications in the processing of image. It helps in decomposing a matrix with a little truncate error according to (2)

$$I=UDV^T \qquad (2)$$

Where **I** refers to the original matrix, while **D** is a diagonal matrix of the Eigen values of **I, U,** and **V** are orthogonal matrices with dimensions **MxM** and **NxN** respectively, and **T** indicates matrix transposition. In [20], they decomposed the cover image and added the watermark using a scaling coefficient as in (3).

$$D+\alpha W=U_W D_W V_W^T \qquad (3)$$

The multiplication of **U**, $\mathbf{V^T}$ and $\mathbf{D_W}$ results in the marked image $\mathbf{I_W}$:

$$I_W=U\,D_W V^T \qquad (4)$$

The possibility of this arose from the basis that the singular values of (SV) of SVD were highly stable. There was a separation of the cover image into blocks and the SVD application to each block in another approach [22]. The watermark dimension must be proportional to the blocks size with a watermark copy fixed in each block. The method increases the quality of the watermark in terms of resistance against attacks and robustness.

B. Transform Domain Watermarking Schemes

In such a technique, the watermark is joined into the cover image/video field and therefore, does not influence the quality of the selected video or image directly. The most commonly used transforms include Discrete Wavelet Transform (**DWT**) Discrete Cosine Transform (**DCT**), and Discrete Fourier Transform (**DFT**). The embedment of the watermark occurs evenly in the general domain of the initial information. The transformation methods initially help in converting the host video/image into frequency domain. The information of the watermark is stored in form of transformed field coefficients. In the end, the application of the inverse transform helps in obtaining the watermarked image/video. Many kinds of research focused on using the DWT because of the multi-resolution characteristics [2]. The DWT gives both frequency and spatial domain features and this makes it Human Visual System (HVS) compatible. Moreover, the DWT helps in enhancing invisibility and robustness when combined with other algorithms.

Discrete Cosine Transform (DCT):

This transform (DCT) has introduced by [23] and has been used and studied extensively since. It is an orthogonal transform, used widely in the processing of images due to its computational efficiency and its energy compaction property. The idea that informs the orthogonal transforms is the need to convert the image to a new domain where it is represented ideally by uncorrelated coefficients, of which very few carry significant energy, and the remaining ones can be quantized to zero to noise ratio but is also more robust against various attacks like frame dropping and frame averaging. Typical steps of DCT watermarking based techniques found in the literature [10, 25] are described hereafter divide the image into a typical 8x8 non-overlapping blocks.

1) For each 8x8 block, apply forward DCT.
2) Selectively, select some blocks based on predefined selection criteria.
3) From selected blocks, identify some coefficient, based on coefficient determination method.
4) Implant watermark by amending the selected coefficients
5) Apply inverse DCT transform on every block.

Discrete Wavelet Transform (DWT):

Discrete wavelet transforms (DWT) [15] has achieved considerable concentration in several signal processing programs, which also includes image watermarking. The undermining theory behind DWT comes from a series of resolution analysis [26] that decomposes the image into a band-limited components set that can be re-used to reconstruct the original image exactly.

One of its main advantages is the likeliness of the structure of data, which obeys the resolution and prevailing decomposition at all levels. At level-1 of DWT, the decomposition of an image is into four sub-bands denoted **LL**(lower resolution approximation image), **LH**(vertical), HL(horizontal), and **HH**(diagonal), where **LH**, **HL**, and **HH** represent the finest scale wavelet coefficients, and LL is the coarse-level coefficients. This process of decomposition is repetitive to enable the calculation of multiple scales. There is a continuous decomposition process until the required scale levels values are determined. Due to the sensitivity of the human eye to the low frequency part (LL sub-band), embedding of the watermark may be in other three sub-bands in retaining desirable quality of the image [27, 29]. Figure 4 shows two levels of the wavelet transform.

As introduced in [29], DWT-based watermarking techniques utilized the spatial information and the frequency the transformed data information to gain robustness. Embedding watermarks in three sub-bands (LH, HL, HH) allows the watermarking techniques to increase its robustness without the noticeable impact of the original image quality. the most natural implementation of the DWT-based watermarking is to use the CDMA sequence in the detail bands as in (5)

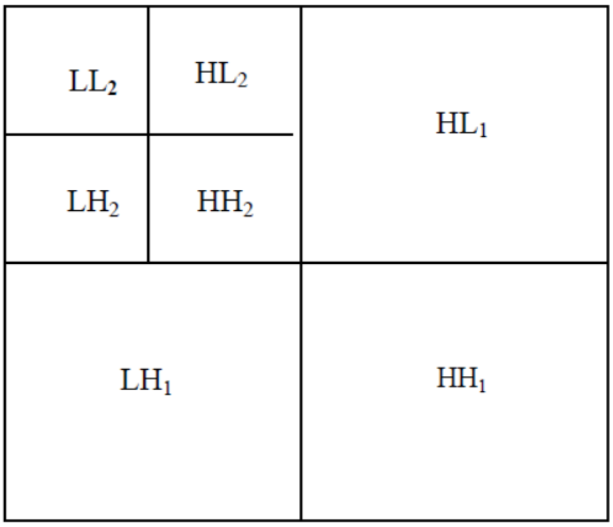

Fig. 4 Two levels DWT

$$I_{w_{u,v}} = \begin{cases} W_i + \alpha |W_i|_{X_i} \,, & U,V \in HL, LH \\ W_i & U,V \in HH, LL \end{cases} \qquad (5)$$

Where **W$_i$** is the wavelet coefficient of the image, **X$_i$** is a watermark bit, and **α** is the scaling factor.

C. Hybrid Domain Watermarking Schemes

In such hybrid domain watermarking techniques, different literature tries to merge between earlier domains for appreciation of the overall effectiveness of the watermarking technique.

SVD-DCT based watermarking:

Sverdlov et al. [30] introduced a new combined approach based on DCT and SVD that is proved buoyant to the diversity of attacks. The algorithm steps are summarized as follow:

1) DCT application to the complete cover image.
2) Zig-zag sequence usage, mapping of the DCT coefficients to the four quadrants.
3) Apply SVD to every separation. These four separations represent minimum to maximum frequency bands.
4) Use the single DCT-transformed visual watermark values to amend the singular every separation of the cover image values.

SVD-DWT based watermarking:

Ganic and Eskicioglu [31] proposed an SVD-DWT based watermarking technique, which is similar to [39] discussed earlier. SVD-DWT main steps are:

1) Apply 1-level DWT on the cover image that will decompose the cover image into 4 sub-bands.
2) SVD application on each sub-band of the cover image.
3) Use the single DWT-transformed visual watermark values to amend the singular every separation of the cover image values.

Watermarks extractions from every sub-band and the respective Pearson correlation coefficient values with the unique watermark image has been documented, which indicates that obtained watermark from the LL band provides the best visual quality and correlation value. This technique has a concern about its performance since its robustness against histogram equalization, sharpening, and contrasting is not very good.

IV. VIDEO WATERMARKING

Video watermarking has some properties that make it different from the watermarking of the other digital contents. Since the video is consist of a sequence of provisional progressive images, however, in fact, we can't consider it as simple as a combination of images, because the nearby frames have both high correlation and a significant amount of temporal and spatial redundancy. Consequently, video watermarking is not only similar to the image watermarking in some characteristics like robustness, security, imperceptibility and watermark capacity, but also has its characteristics, such as processing is done in real time, constant code rates, random detection, and the ability to be used along with standards of video coding. Generally, in different applications, watermarking techniques need to achieve different requirements. Performance in the video watermarking technique is evaluated by analyzing their robustness, real-time processing, watermark capacity, and imperceptibility. Additionally, for watermarking techniques in the compressed domain, a bit increase rate (BIR) may be assessed as one of the performance metrics.

video watermark embedding algorithm has different types according to the embedding position; the following is the main types of video watermark embedding algorithm [1]:

1) **Original Video-Based Watermarking:** where the original video is perceived as a sequence of static images and watermark data is embedded into the original image, and then the watermarked video is recompressed. The main advantage of the algorithm include

a) is not dependent on the video **compression** techniques.

b) its implementation is **simple**, and we can re-use many watermarking schemes introduced initially for static images.

This original video-based watermarking has some **drawbacks**:

a) We have to **decode** the compressed host video before embedding and **encode** it back after finishing the watermark embedding.

b) To extract the watermark, we have to do complete decoding, which is **very costly**.

c) If the video goes for compression with a high compression ratio, the embedded watermark can be **removed easily**.

2) **Encoding process-based video watermarking algorithm**: watermark embedded by utilizing redundant spaces of the video in the process of compression coding, including motion vectors, quantized DCT coefficients, ... etc. **Advantages** of this algorithm are:

a) using quantized coefficients to embed watermark is **efficient** and **straightforward**, with minor impact on the code rate of video streams.

b) the embedding process can be combined with the standard video coding. Thus, the watermark can be embedded and **extracted in real-time**.

Video watermarking algorithms in the encoding process has some drawbacks:

a) limited embedding capacity since the video coding parameters impacts it.

b) we have to modify the encoder and decoder, which may limit the introduction of some watermarking techniques.

3) **Post Compression Video Watermarking**: Embedding algorithm try to find redundant space in the compressed bitstream and embed the watermark information into it. The **advantage** of this algorithm:

a) efficient and independent of the corresponding codec.

b) high fidelity and computational redundancy are small.

Post compression video watermarking **drawbacks**:

a) limited capacity due to limited availability of the redundant space for watermark embedding.

b) poor robustness.

A. Visible Watermarking Embedding

The Visible Watermarking Embedding process enables the perceptive insertion of a watermark W into an original video/image V so that the watermark is visible by the human vision system (HVS). The objective of visible watermarks is to be noticeable without a vital effect on the quality of the original video/image. However, most of the visible watermarks are irreversible, and thus authenticated users cannot reconstruct the original content of video/image with the same quality after watermark extraction. This introduces a limitation in different applications like medical, military, and law. from this point, a need to have a reversible visible watermark is raised.

Recently, in [32], a new visible watermarking technique using Seam Carving [33] to be robust against inpainting. Seam Carving is an efficient algorithm for resizing images adaptively. Where they are doing resizing of the image by duplication or repeating a seam, that is represent the optimal path of the pixels having minimum energy from left to right in case of vertical adjustment or top to bottom in case of horizontal adjustment. In the literature, There is multiple **reversible visible** watermarking approach that can be used for such application as in [34, 35, 36, 37] but, these approaches are sensitive to quantization errors introduced by standard image/video compression standards. Thus, these approaches are not appropriate for most Internet applications where video content needs to be compressed in prior real-time transmission.

B. Video Encoder

Many of the visible watermarking techniques depend on the structure of the used video encoder. The Video Encoder process utilizes the H.264/AVC standard encoder to compress the provided video.

The process of encoder utilizes motion estimation and spatial pre-determination to ensure maximization of residual faults to be encoded. The encoder calculates the residual data to be encoded by computing the difference between the original frame and the predicted one. Using DCT, The consequential residual data is de-correlated and labeled ensure the minimum possible protection of valuable data and still realize adequate standards of image quality. The quantized converts coefficients are then inverse quantized and inverse transformed to recover the residual error **E,** which also involves the quantization error generated by the lousy property of the average video codec. Reuben A. Farrugia [38] suggested a contemporary reversible visible watermark, which uses two Video Encoder processes. In the first encoder process, they receive the watermarked frame I_W, computes motion prediction, and spatial estimation to compress the video. in the second process, the encoder receives the original video stream **I** and compresses it using the **motion vectors**.

V. QUALITY ASSESSMENT FOR VISIBLE WATERMARKING EMBEDDING SCHEMES

The HVS that is used to measure quality generates subjective value scores according to the regulated environment, such as display resolution and viewing distance. In the past decade, several mechanisms have been proposed to defined perceptual metrics. The metrics defined a distortion threshold above which the HVS will notice the impact of the watermark. Structural similarity metrics (SSIM), is one of the widely used metrics. While Mean Square Error (MSE) and classical perceptual metrics change with changes in contrast, intensity, spatial, and scale adjustments. On the contrary, the SSIM considering the idea that HVS is designed for processing structural data (relative spatial covariance) from images. Thus, experts recommend the study of objective mechanism which is helps to evaluate the quality of an image important to study the objective mechanism for the evaluation of image quality for variable visible watermark technologies, which depend on models of visual ideas. The table below provides a list of different quality metrics applicable in evaluating the visible watermarking schemes [39]:

Metric	Description
Mean Squared Error(MSE)	Determines the standard 'error' square, where error refers to the quantity provided by the estimator from the amount that needs to be determined.
Information Fidelity Criterion (IFC)	The quantity of the data distorted image offers about the original.
Noise Quality Measure (NQM)	According to the Peli's contrast
Peak Signal-to-Noise Ratio (PSNR)	Ratio of the highest possible power of an image and the power of reconstructed noise
Signal-to-Noise Ratio (SNR)	Ratio between average signal powers to average noise power
Structural Similarity Metric (SSM)	Measure the likelihood between two images
Mean SSIM (MSSM)	the average of value of SSIMs
Universal Quality Index (UQI)	Approximation of quality index from a local setting
Visual Information Fidelity (VIF)	Concerns local collective data, which determines the amount of information capable to transmit from the reference image to the human server
pixel-based VIF (VIFP)	multi-scale pixel domain implementation of VIF

VI. RESULT AND DISCUSSION

Spatial domain based-watermarking techniques are widely used due to its simplicity. However, it still suffering from robustness issues against illegal attacks. Table 1 is comparing the main watermarking methods based on the spatial domain.

In transform-based watermarking techniques, the host image or video is transformed to the frequency domain, then the watermark pattern is embedded using the embedding technique. The main advantage of this technique is it robustness, however it has limited capacity. Table2 give a comparison between the main transform-based techniques.

In transform-based watermarking techniques, the host image or video is transformed into the frequency domain; then, the watermark pattern is embedded using the embedding technique. The main advantage of this technique is its robustness. However, it has limited capacity. Table 2 gives a comparison between the main transform-based techniques.

The hybrid transform-domain techniques exploit the strengths of different transformers in order to enhance the total performance of the watermarking system.

Table I Spatial-Based watermarking typical techniques

Spatial-based Watermarking				
Method	Watermark type	Image/ video	Watermark	Embedding
I. Bayoudh, S. Jabra and E. Zagrouba [41]	Blind-invisible	Video	Encoding Watermark before embedding	Use dynamic multi-sprites
Z. Bahrami, and F. A. Tab [42]	Semi-blind - invisible	Video	Raw , embedded pixel by pixel.	Based on key frames and block classifications
R. Liu and T. Tan [21]	invisible	Image	Watermark same dimension as image	SVD based-embedding. high probability of false-positive

Table II Transform-Based watermarking typical techniques

Transform-based Watermarking				
Technique	**Watermark type**	**Image/video**	**Watermark**	**Embedding**
Singh and K.M [43]	Invisible-blind	Video	Apply **Arnold** transform on the watermark	DWT based embedding - Y-component
K.R. Espinoza, E. F-Navarro, C. C-Ramos [33]	visible	Image	Use Seam carving to generate watermark pattern	DCT -based
S. Gaj, A.K. Rathore[44]	Invisible-blind	video	No pre-processing	**Hybrid**, DCT and SIFT

VII. CONCLUSION

In this paper, the research goal is to offer a simple framework of the digital watermarking technology. The digital watermark can actually include the issue of copyright protection for digital content. Keeping the security of the watermarking is a big challenge. From this overview, it is found that the hybrid watermarking embedding systems are more secure against potential breaches. As a prerequisite of the visible watermark embedding process to preserve the initial image details, the watermark pattern should be in simple shapes and textures. In case the watermark shapes are distorted without a significant impact on the original hosted image, the authorized owner will not be able to proof its own against the illegal attacks. Therefore, we should be possible to draw the self-identified structures from the watermark image.

REFERENCES

1. Xiaoyan Yu, Chengyou Wang, and Xiao Zhou, "A Survey on Robust Video Watermarking Algorithms for Copyright Protection", MDPI Journal, Appl. Sci. 2018, 8, 1891; doi:10.3390/app8101891, 2018.
2. A. A. Hood and Prof. N. J. Janwe, "Robust Video Watermarking Techniques and Attacks on Watermark – A Review", International Journal of Computer Trends and Technology, vol. 4, Issue No. 1, 2013.
3. Ekta Miglani, Sachin Gupta "Digital Watermarking Methodologies - A Survey", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, May 2014.
4. G. Kaur and K. Kaur, "Digital Watermarking and Other Data Hiding Techniques", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Vol. 2, Issue No. 5, April 2013.
5. N. H. O. A. K. K. Adesina A.O., "Digital watermarking: A state-of-the-art review," in 2010 IST-Africa, 2010
6. C. I. Podilchuk and E. J. Delp, "Digital watermarking: algorithms and applications," Signal Processing Magazine, IEEE, vol. 18, no. 4. pp. 33-46, 2001.

7. A. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, Second Edi., Burlington: Morgan Kaufmann, pp. 425-467, 2008
8. Prabhishek Singh, R S Chadha, “A Survey of Digital Watermarking Techniques, Applications and Attacks”, Proceedings of International Journal of Engineering and Innovative Technology (IJEIT), March 2013.
9. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom "Digital Watermarking and Steganography" Second Edition, Morgan Kaufmann Publishers, 2008.
10. I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography. Morgan Kaufmann, 2008.
11. J. Liu and X. He, “A review study on digital watermarking,” First International Conference on Information and Communication Technologies, pp. 337–341, 2005.
12. [12] M. Arnold, M. Schmucker, and S. D. Wolthusen, Techniques and Applications of Digital Watermark and Content Protection. Artech House, 2003.
13. X. Wu, J. Hu, Z. Gu, and J. Huang, “A secure semi-fragile watermarking for image authentication based on integer wavelet transform with parameters,” Australasian Information Security Workshop, vol. 44, 2005.
14. M. El-Gayyar and J. von zurGathen, “Watermarking techniques spatial domain,” University of Bonn Germany, Tech. Rep., 2006.
15. M. Antonini, M. Barlaud, P. Mathieu, and I. Daubechies, “Image coding using wavelet transform,” IEEE Transaction on Image Processing, vol. 1, pp. 205–220, 1992.
16. A. Daubechies and W. Sweldens, “Factoring wavelet transforms into lifting steps,” SIAM Journal on Mathematical Analysis, 1997.
17. C. Podilchuk and E. Delp, “Digital Watermarking Algorithms and Applications”, In IEEE Signal Processing Magazine, vol. 18, Issue No. 4, pp. 34-46, July 2001.
18. N. Pantuwong and N. Chotikakamthorn, “Line watermark embedding method for affine transformed images,” ISSPA 2007, pp. 1–4, 2007.
19. S. Riaz, M. Y. Javed, and M. A. Anjum, “Invisible watermarking schemes in spatial and frequency domains,” International Conference on Emerging Technologies, 2008.
20. S. Patel, A. K. Katharotiya and M. Goyani, “A Survey on Digital Video Watermarking”, International Journal Comp. Tech. Appl., Vol. 2 (6), pp. 3015-3018, Nov. - Dec. 2011.
21. R. Liu and T. Tan, “An svd-based watermarking scheme for protecting rightful ownership,” IEEE TRANSACTIONS ON MULTIMEDIA, vol. 4, pp. 121–128, 2002.
22. R. A. Ghazy, N. A. El-Fishawy, M. M. Hadhoud, M. I. Dessouky, and F. E. A. E.-S. Samie, “An efficient block-by-block svd-based image watermarking scheme,” National Radio Science Conference, pp. 1–9, 2007.
23. Ahmed Nasir, Natarajan T., Rao K. R. " Discrete Cosine Transform ", IEEE Transactions on Computers, C-23 (1): 90–93, doi:10.1109/T-C.1974.223784 , 1974.
24. Ekta Miglani, Sachin Gupta "Digital Watermarking Methodologies - A Survey", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, May 2014.
25. N. A. Shelke and Dr. P.N. Chatur, “A Survey on Various Digital Video Watermarking Schemes”, International Journal of Computer Science & Engineering Technology (IJCSET), Volume 4, Issue 12, Dec. 2013.
26. V. M. Potdar, S. Han, and E. Chang, “A survey of digital image watermarking techniques,” 3rd IEEE International Conference on Industrial Informatics, pp. 709–716, 2005.
27. S. Mallat, "The theory for multiresolution signal decomposition: The wavelet representation", IEEE Trans. Pattern Anal. vol. 11,no. 7, pp. 654–693, Jul. 1989.
28. G. Langelaar, I. Setyawan, R.L. Lagendijk, "Watermarking Digital Image and Video Data", in IEEE Signal Processing Magazine, Vol 17, pp 20-43, 2000.
29. Chih-Chin Lai, Cheng-Chih Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE transaction on instrumentation and measurement, vol. 59, no. 11, 2010.
30. C. S. Woo, J. Du and B. Pham, " Performance Factors Analysis of a Wavelet- based Watermarking Method ", Proc. 3rd Australasian Information Security Workshop (AISW2005), CRPIT, vol. 44, pp. 89-97, 2005.
31. A. Sverdlov, S. Dexter, and A. M. Eskicioglu , " Robust DCT-SVD Domain Image Watermarking for Copyright Protection: Embedding Data in All Frequencies ", Multimedia Computing and Networking 2005 Conference, 2005.
32. E. Ganic and A. M. Eskicioglu, " Secure DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies", ACM Multimedia and Security Workshop 2004.
33. Kevin Rangel-Espinoza, Eduardo Fragoso-Navarro, Clara Cruz-Ramos, Mariko Nakano-Miyatake, Manuel Cedillo-Hernandez, and Hector Perez-Meana, "Visible Watermarking Robust against Inpainting Using Seam Carving , ", 7th International Workshop on Biometrics and Forensics (IWBF), IEEE, 2019.
34. Zheng. X.S., Zhao. Y.L., Li. N, " Classification model and enhancement of robustness in video digital watermark.", In Proceedings of the Chinese Control and Decision Conference, Yantai, China, 2008.
35. Y. Yang, X. Sun, H. Yang, C.-T. Li, and R. Xiao, "A contrast sensitive reversible visible image watermarking technique", Circuits and Systems for Video Technology, IEEE Transactions, 2009.
36. Hu and B. Jeon, “Reversible visible watermarking and lossless recovery of original images,” Circuits and Systems for Video Technology, IEEE Transactions, vol. 16, no. 11, 2006.
37. S.-K. Yip, O. Au, C.-W. Ho, and H.-M. Wong, “Lossless visible watermarking", in Multimedia and Expo, 2006 IEEE International Conference, 2006.
38. H.-M. Tsai and L.-W. Chang, “A high secure reversible visible watermarking scheme,” in Multimedia and Expo, 2007 IEEE International Conference, pp. 2106 –2109, 2007.
39. Reuben A. Farrugia, "Reversible Visible Watermarking for H.264/AVC Encoded Video", Department of Communications and Computer Engineering, University of Malta, Msida, 2011.
40. Min-Jen Tsai and Jung Liu , "The Quality Evaluation of Image Recovery Attack for Visible Watermarking Algorithms", Institute of Information Management, National Chiao Tung University, R. O. C, 2010.
41. I. Bayoudh, S. Jabra and E. Zagrouba," Online multi-sprites based video watermarking robust to collusion and transcoding attacks for emerging applications", Multimed Tools Appl, DOI 10.1007/s11042-017-5033-y, 2018
42. Z. Bahrami, and F. A. Tab, "A new robust video watermarking algorithm based on SURF features and block classification", Multimed Tools Appl, DOI 10.1007/s11042-016-4226-0, 2018
43. Singh and K.M. "A robust rotation resilient video watermarking scheme based on the SIFT,", Multimedia Tools Appl. 2018.
44. S. Gaj ;, A.K. Rathore; A. Sur; Bora, and P.K " A robust watermarking scheme against frame blending and projection attacks". Multimedia Tools Appl. 2017.

AUTHORS PROFILE

A. Al. Embaby was born in Beheira, Egypt in 1981. He received the B.S. and M.S. degrees in information technology from Cairo University, Giza, in 2012. From 2014 he is a PhD student in Faculty of Computers and Artificial Intelligence, Cairo University, Giza.

From 2003 to 2005, he was a satellite Mission Analysis engineer with Yuzhnoy State Design Office, Dnepropetrovsk, 49008, Ukraine. From 2003 to 2008, he was a Satellite System Engineer with the National Authority for Remote Sensing & Space Sciences (NARSS), Cairo, Egypt. From 2008 to 2015, he was a Software development Team Leader at MAIDIS International, Abu Dhabi, UAE. Since 2016 he is a Technical manager at Second Step Software Development LLC, Abu Dhabi, UAE. His research interest includes developing multimedia and image processing techniques using machine learning and AI, development of mission and space system software, developing healthcare information system and Learning Management System.

Mohamed. A. Wahby Shalaby received the BSc. and MSc. degrees in computer engineering from Cairo University, Egypt, in 1997 and 2002, respectively, and the PhD degree in electrical and computer engineering from Concordia University, Canada in 2012. Starting from 2103 till 2017, he was a full-time assistant professor in the fields of robotics, image and video processing at the information technology department, faculty of computers and artificial intelligence, Cairo University, Giza, Egypt. Then he joined the mechatronics program at faculty of engineering and applied sciences, Nile University, Giza, Egypt.

His research interests include robotics, artificial intelligence, deep learning, biometrics, image processing, pattern recognition, and computer vision.
Dr. Shalaby has been an associate editor of the Egyptian Informatics Journal, Elsevier, since 2015. Recently, Dr. Shalaby has been a founding member of the multi-disciplinary Smart Engineering Systems Research Center (SESC) at Nile University, Giza, Egypt