IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 9, 2021, accepted February 17, 2021, date of publication February 22, 2021, date of current version March 2, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3060861

Hybrid SVD-Based Image Watermarking Schemes: A Review

WAFA' HAMDAN ALSHOURA[1], ZURINAHNI ZAINOL[1], JE SEN TEH[1], MOATSUM ALAWIDA[1], AND ABDULATIF ALABDULATIF[2], (Member, IEEE)

[1]School of Computer Sciences, Universiti Sains Malaysia, Gelugor 11800, Malaysia
[2]Department of Computer Science, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia

Corresponding authors: Wafa' Hamdan Alshoura (wafahamdan@student.usm.my), Zurinahni Zainol (zuri@usm.my), and Je Sen Teh (jesen_teh@usm.my)

This work was supported by the Universiti Sains Malaysia, and in part by the Research University Grant under Grant 1001/PKOMP/8014074.

ABSTRACT Watermarking is an important technique for protecting sensitive e-multimedia data and intellectual property. Watermarking techniques are used for many applications such as ownership protection, which is a popular area of research as compared to others such as authentication and local temper localization. There are many image watermarking schemes that have been recently published based on the frequency domain as it can fulfill watermarking requirements such as high robustness and imperceptibility. Singular-value decomposition (SVD) is one of them and is used in many frequency transform-based image watermarking schemes due to its stability and mathematical simplicity. However, there are many schemes that lack robustness against malicious cyberattacks, whereby the watermarks are easy to detect and destroy. Consequently, the proposed watermarking schemes became more complicated and cannot resist various geometric and non-geometric attacks. Thus, there are many existing hybrid SVD-based image watermarking schemes found be insecure. As there is also a lack of in-depth reviews in this domain, the focus of this paper is the analysis of the state-of-the-art in hybrid SVD-based image watermarking. We perform efficiency comparisons to highlight various security problems, open issues, and research gaps. Based on our findings, we additionally provide some recommendations for the development of more robust schemes in the future. This paper provides essential information for researchers and practitioners alike to advance the field of image watermarking.

INDEX TERMS Embedding, extraction, frequency domain, image watermarking, singular-value decomposition (SVD).

I. INTRODUCTION

Digital data (such as text, video, audio, and image) are transmitted over open channels such as the Internet which invariably makes the protection of private data and intellectual property rights (IPR) to be extremely important in this era [1]–[6]. Digital data types can be easily converted, altered, copied and widely distributed while preserving high quality. It is difficult to save real ownership and copyright of digital data because an adversary (e.g., hacker, attacker, and pirate) may violate it. An adversary can manipulate, reproduce, alter, modify, re-transmit digital data over the Internet, and prove the ownership. Data or multimedia encryption (cryptography) is a method to protect sensitive data and the ownership of digital data while in storage or transmission. However, encryption focuses on protecting data itself instead of proving ownership [7].

In a general context, cryptography provides strong protection for digital content with limited distribution, and authorized parties have the full right to handle secret data after the decryption process [8]. However, cryptography has faced the challenge of distributing digital data while protecting the ownership/copyright of the content. In order to overcome the challenge of using cryptography in proving ownership, the data hiding method is used to embed the message in the digital content before it is distributed. Hence, data hiding using processes such as watermarking is an intelligent technique that saves the original owner of the digital data by protecting

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

it against illegal copying or distribution or to send secret information to other parties (Stenography) [9].

Watermarking is a technique that can preserve copyright, maintain content authentication, copy control and protect the digital content after the decryption process. This paper encapsulates how the concept of image watermarking is leveraged as an alternative technique to protect digital image over image encryption. The image watermarking technique can achieve a set of necessary requirements of protecting the digital image (such as copyright, authentication, tamper localization, recovery image, and so forth) [10], [11]. Many image watermarking schemes have been proposed in different image applications in recent years [12]–[16]. However, some of these schemes have remained impractical due to some challenges and limitations in their designs [17], [18].

A hybrid image watermarking scheme is based on two or more frequency domains [19], [20]. Frequency domain has garnered more attention than spatial domain [21]. Spatial domain focuses to alter the image pixel directly, where frequency transform changes image pixels to frequency coefficients and then manipulated them. Frequency-only embeds a watermark by altering frequency coefficients after applying a frequency transform. The newly altered coefficients are inverse to the spatial domain. Hybrid image watermarking schemes have been largely proposed to face the limitations in spatial-only and frequency-only image watermarking scheme [22], [23]. SVD is used in many hybrid image watermarking schemes due to has set of advantages such as simplicity and stability [19], [24]–[30] and is used in video watermarking schemes [31]–[35]. However, there are a lot SVD-based image watermarking schemes found to be insecure and inefficient, whereby an adversary can easily destroy and extract a fake watermark signal from the watermarked image [18]. The limitations that can be found in existing schemes are summarized as follows:

- Most embedding processes are performed on singular values because of low distortions and high robustness against different attacks. However, these methods are susceptible to the false positive problem (FPP) attacks.
- Most watermark encryption methods use scrambling algorithms, which rely on Arnold and logistic chaotic maps. These maps are not enough secure.
- Most existing schemes used side information generated during the embedding process for extraction. Side information should be protected and should not consist of sensitive values used for embedding watermark images.
- The singular vectors of the host and watermark images are highly sensitive to tiny changes, and will adversely affect the quality of the watermarked image and extracted watermark if used in the embedding process.
- The use of colored host and watermark images with SVD transform still require more studies.
- Current solutions proposed to avoid FPP attacks need additional authentication processes such as the use of digital signature and hash value.
- Optimal scaling factors that were used to achieve a better balance between watermark requirements lead to computational overheads and are limited in scale. Moreover, their values need to be stored for the extraction process.

In this paper, we review hybrid SVD-based image watermarking schemes to display all limitations and challenges. The novelty of this paper lies in its critical analysis of eight comparative factors of the existing hybrid SVD-based watermarking schemes. In addition, over 70 SVD-based schemes are carefully studied and included in our analysis to correctly highlight future directions for readers. Initially, we introduce the data hiding types, watermark applications and its requirements. To clarify the difference between different domains and types of watermarks, the classification of digital watermarks is introduced. To demonstrate the limitations and research gaps in the existing SVD-based image watermarking schemes, these existing schemes are analyzed on overall directions such as embedding methods, watermark size, scale factor and others. We then highlight a set of research gaps based on the performance comparison of the existing schemes. Finally, a set of recommendations is provided to facilitate the design of improved watermarking schemes. The list of contributions of this paper are as follows:

1) Background of data hiding and watermarking applications are provided to make the paper integrated and reader-inclusive.
2) New analysis and critical comparison of hybrid SVD-based image watermarking schemes are included to help researchers develop new SVD-based image watermarking schemes.
3) Limitations, challenges and research gaps of hybrid SVD-based image watermarking schemes are highlighted.
4) Research recommendations and directions are presented to assist developers and researchers in their future work.

The remaining sections of this paper are as follows: Section II provides related work on related survey or review papers in the field. Then, the various data hiding types are detailed in Section III, followed by image watermarking requirements and applications in Section IV. Classification of digital watermarking schemes are provided in Section V. More details on existing hybrid SVD-based image watermarking schemes are introduced in Section VI. Comparison and critical analysis of these schemes are provided in Section VIII. Research gaps and discussion with recommendations are detailed in Sections IX and X, respectively. Section XI provides some final remarks and a summary of findings to conclude the paper.

II. RELATED WORK

Over the years, there have been a number of surveys that study watermarking in various data type domains but do not provide an in-depth look at SVD schemes [7], [36]–[42]. There are surveys that look into the security aspects of the existing SVD

watermarking schemes but do not analyze the vital research gaps in the area [18]. Many schemes have been proposed based on SVD along with one or more frequency transforms [19], [24]–[30], [43]–[46]. These schemes are referred to as hybrid SVD watermarking schemes, and still need to be further studied to identify existing limitations and challenges.

Kumar *et al.* [36] wrote a survey on multimedia and database watermarking schemes. They reviewed different watermarking multimedia types, and analyzed them to aid researchers in designing new multimedia watermarking schemes. The survey presents a broad background on watermarking requirements, detailed classifications, various attacks on watermarking, and summary of number state-of-the-are watermarking schemes. Singh *et al.* [37] introduced a survey on soft computing image watermarking approaches for several applications. The survey studied the fundamental principles of watermarking and soft computing techniques that were applied in the embedding stages in watermarking. This includes Neural Networks (NN), Genetic Algorithms (GA), Support Vector Machines (SVM), Principal Component Analysis (PCA), Meta-Heuristic approaches, Deep learning (DL) and Fuzzy Logic (FL). Some of major issues in the state-of-the-art of soft computing-based watermarking schemes were discussed.

Evsutin *et al.* [38] reviewed data hiding approaches (steganography and watermarking) for digital images. The survey focused on the current trends of the data hiding algorithms, and the challenges in steganography and watermarking areas. Performance comparison between watermarking and steganography schemes was provided, related to the different information embedding methods in digital images. In addition, some of the current research trends were discussed. Kumar *et al.* [39] presented a summary of the different state-of-the-art watermarking strategies, along with a performance comparison and a discussion on open issues. The solutions presented in the paper are useful for the researchers who interested to secure e-governance applications.

In their survey, Khan *et al.* [7] covered recent state-of-the-art in reversible watermarking schemes. Reversible watermarking is used to restore the cover work (image, video or text) after full extraction of the embedded watermark. This has many applications such as in healthcare and law-enforcement. Their paper included a discussion on the basic concepts of watermarking, detailed performance analysis and experimental comparison of various schemes. A dataset of 300 images was used in the experimental comparison where computational time and watermark properties were used as comparison criteria. The paper also forecast future trends in the area for researchers to pursue. Singh *et al.* [40] presented a summary of different aspects of secure digital image watermarking approaches. Their survey studied the cryptography techniques used in designing watermarking schemes such as chaotic maps, homomorphic cryptosystem, visual cryptography, hash functions and public-key cryptography.

Mousavi *et al.* [41] presented a survey on medical image watermarking techniques. An overview of watermarking strategies was provided, followed by a study of the security, advantages and disadvantages of medical image watermarking schemes. Schemes based on frequency transforms were the focus of their paper. Agarwal *et al.* [42] reviewed robust and imperceptible watermarking schemes in the spatial and transform domain. The authors studied a number of factors used for image watermarking such as robustness, security, imperceptibility and others. They also examined different techniques used to develop image watermarking scheme. The authors conclude that robustness is enhanced when techniques such as data mining, NN, GA, and others were used. Analysis and comparison revealed research challenges for image watermarking, for which the authors presented some solutions. To date, these survey and review papers do not focus on hybrid SVD watermarking scheme for images.

Makbol *et al.* [18] studied hybrid SVD-based watermarking schemes under three FPP scenarios. Several watermarking schemes were analyzed and classified based on the likelihood of being susceptible to FPPs. Three FPP attacks and their corresponding solutions were reviewed. Reliability tests to analyze the security aspects of existing schemes were also conducted. Their analysis demonstrated that a large number of hybrid SVD-watermarking schemes suffer from FPP, and some of the existing solutions have limitations. However, this paper only focuses on FPP and does not look into other research challenges nor crucial factors that have an impact on the field. Ahmadi *et al.* [47] presented a survey of SVD-based watermarking schemes for digital images. The survey studies 30 existing SVD schemes and compares them based on objectives, frequency transforms, artificial intelligent approaches, type of embedding strategy, modifying SVD components, capacity, importance, and watermark type and size. Significant problems and their solutions were discussed. However, the survey does not cover other SVD-based watermarking schemes and their research challenges. In addition, some schemes such as zero and singular vector embedding were not covered.

We bridge the gaps of existing survey papers by analyzing a large number of SVD-based watermarking schemes based on various perspectives. Previous survey and review papers only cover a limited number of watermarking schemes and data hiding methods. This paper covers 60 existing hybrid SVD-based watermarking schemes. An in-depth comparison of these schemes reveal research gaps and challenges that researchers can delve into. Finally, we introduce some recommendations that should be taken into consideration for future work in the area. Table 1 provides a comparison of existing surveys, including ours.

III. DATA HIDING TYPES

The data hiding technique is an approach used to hide messages or data into a host or cover medium (multimedia). The embedded data is preserved by leveraging various distortion operations on the cover medium that may result from

TABLE 1. Comparison of survey papers.

Survey paper	Applications and multimedia type	Number of compared schemes	Coverage of SVD watermarking	Research gaps for SVD schemes	Watermarking requirements discussed
Ref. [36]	Watermarking (different multimedia types)	20 (image watermarking)	No	Yes (FPP, computational cost)	Robustness, imperceptibility, security and capacity
Ref. [37]	Watermarking (digital image)	56 (soft computing-based image watermarking)	No	NO	Robustness, imperceptibility and capacity
Ref. [38]	Watermarking and Steganography (digital image)	31 (image watermarking)	No	No	Robustness and imperceptibility
Ref. [39]	Watermarking (digital image)	45 (image watermarking)	Yes	Yes (FPP, embedding capacity)	Robustness and security
Ref. [7]	Reversible watermarking (different multimedia types)	24 (reversible schemes)	No	No (prediction-error expansion and tamper localization issue)	Robustness, imperceptibility, capacity, computational time and security
Ref. [40]	Watermarking. (digital image)	30 (image watermarking)	No	No	Security
Ref. [41]	Watermarking (medical image)	6 (image watermarking)	No	No	Robustness, imperceptibility, reversibility, authentication and fragile
Ref. [42]	Watermarking (different multimedia types)	50 (multimedia watermarking)	No	No	Robustness, imperceptibility, security and capacity
Ref. [18]	Watermarking (digital image)	23 (image watermarking)	Yes	FPP	Security
Ref. [47]	Watermarking (digital image)	30 (image watermarking)	Yes	Yes (FPP and embedding color image)	Robustness, imperceptibility, security and capacity
Our Survey	Watermarking (digital image)	60 (image watermarking)	Yes (frequency domain + SVD)	Yes (MSF without AI optimization algorithms, Overcome FPP without extra authentication, and lack of security properties)	Robustness, imperceptibility, security and capacity

transmission noises or attacks by adversaries. Nevertheless, there are many constraints that drive and control the data hiding operation [8] which are: the capacity of data to be embedded (payload, quantity), the ability of the embedded data to be uniform under many distortions of a cover medium (host), and the capability of the embedded data to be immune to interception, modification, or removal operations by a third party.

Most of the data hiding techniques found in literature can be categorized into two groups namely: digital watermarking and stenography [7]. The two groups focus on concealing the existence of a message which is differs from cryptography which focuses on protecting the data content itself. Hence, there are basic differences and design goals for watermarking, stenography and cryptography as summarized in Table 2.

In watermarking schemes, the embedded watermark process has the objective of protecting ownership of the host object by preserving a watermark under different critical conditions [8], [48]. Hence, the priority in watermarking schemes is always given to the robustness property. On the other hand, visual quality of the host object is also another objective, referred to as the imperceptibility property [42]. In some watermarking applications, there is a relationship between watermark and host object such as it can embed a piece of patient information in its medical images [49], [50]. Based on these properties and various applications, the watermarking field has attracted researchers in the last years [40].

A. GENERAL FRAMEWORK OF DIGITAL IMAGE WATERMARKING

Digital images are mediums widely used in digital communication. The digital image format commonly used to evaluate watermarking schemes is the gray level image, where each 8-bit pixel has a pixel intensity ranging between 0 to 255. A gray image is commonly used in experiments because it can be easily processed as compared to coloured images. Hence, the use of gray images has been widely adopted in image watermarking research.

In image watermarking, a watermark is embedded into a digital image known as the host or cover image. This watermark is usually a gray image that may contain a logo or text. There is a set of common phases which formulates the general

TABLE 2. Comparisons between watermarking, steganography, and cryptography [9].

Criterion	Watermarking	Steganography	Cryptography
Host (Cover)	Multimedia file (image, video and audio are preferable)	Multimedia file (image, video and audio are preferable)	Plaintext bits, or block data.
Embedded Data	Watermark	Payload	Stream or block bits
Size of embedded data	Small	Limited based on host's size	No size limits
Main Objective	Copyright	To send secret data	Protect data from unauthorized parts
Input	Two (host and watermark)	Two (host and secret message)	One (plaintext)
Output	Watermarked-object	Stego-object	Ciphertext
Secret Key	Not used in the most of cases, and based on robust systems	Not used in the most of cases, and based on secure stego-systems	Necessary
Visibility	Unknown	Unknown	known
Applications	Intellectual property, copyright protection, and authentication	Secret communication, documents protection against forgery, and Medical imaging	Information exchange protection
Attacks	Image processing, signal attack, and geometric attacks	Steganalysis	Cryptanalysis
Fails when	Removed, altered, and destroyed	Detected	Broken ciphertext

model of image watermarking schemes [51], [52]. These consecutive phases are embedding, distribution, extraction, and decision processes. Figure 1 shows these consecutive phases.

B. WATERMARKING SCHEME EVALUATION

Peak-signal-to-noise ratio (PSNR) and normalized correlation (NC) are the two main tests to assess the imperceptibility and robustness of a watermarking scheme [53], respectively. PSNR can be defined as [18], [47]

$$PSNR = 10\log_{10}\left[\frac{max(I(i,j))^2}{MSE}\right] \quad (1)$$

where $max(I(i,j))$ is the largest pixel value in the host image, while the mean square error (MSE) between the host image I and the watermarked image I^W can be calculated as [18], [47]

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - I^W(i,j)]^2 \quad (2)$$

where M and N are the number of rows and columns of an image. A high PSNR value indicates that there is minimal difference between the host image I and watermarked image I^W. On the other hand, NC is a measure of the difference between an extracted watermark W^{new} and the original watermark W. NC is calculated as [18], [47], (3), as shown at the bottom of the next page, where μ_1 and μ_2 denote the mean values of W and W^{new}, respectively. When the original and extracted watermark image closely resemble one another, $NC \approx 1$. In case where $NC = 1$, the original and extracted watermarks are identical. There are fifteen attacks commonly used to evaluate the robustness of a watermarking scheme. Table 3 summarizes these fifteen attacks whereas Figure 2 visually depicts these attacks in practice.

TABLE 3. Geometrical and non-geometrical attacks and their descriptions.

Attack	Attack description
Cropping	Replace pixels of watermarked images with zero values.
Cutting	Replace rows or columns of watermarked images with zero values.
Shearing	Distort the watermarked image in the x-, y or both directions.
Translating	Translate watermarked images by varying translation coordinates.
Shifting	Shift pixels of watermarked images by a number of rows or columns.
Rotating	Rotate watermarked images a specific number of degrees.
Scaling	Scale the size of watermarked images with scaling factors ranging between [0.6,2.0].
Median Filter	Substitute pixels in watermarked images by the median value of adjacent pixels with a 3×3 mask.
Gamma Correction	Perform gamma correction to the watermarked image.
Wiener Filter	Use a Wiener filter on the watermarked image.
Histogram Equalization	Apply histogram equalization to adjust the contrast watermarked images.
Salt Pepper Noise	Add salt and pepper noise to the watermarked image with a density ranging between [0.001, 0.04].
Speckle Noise	Distort watermarked images using speckle noise with different densities.
Gaussian Filter	Distort watermarked images using Gaussian noise ranging between [0.0001,1].
JPEG Compression	Perform JPEG compression on watermarked images with a ratio between [30%,90%].

IV. IMAGE WATERMARKING REQUIREMENTS AND APPLICATIONS

Digital image watermarking schemes share some common requirements which have been presented alongside their

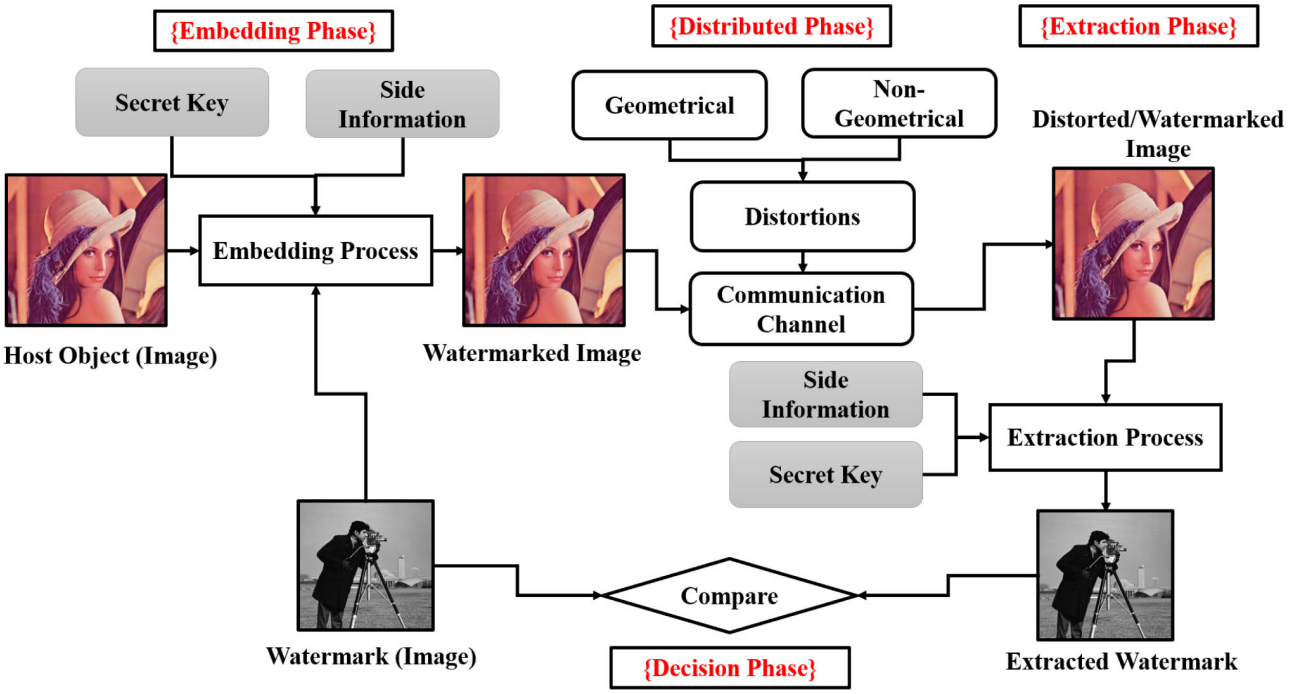

FIGURE 1. General model of watermarking system.

applications [2]. In this section, we delve deeper into these requirements. Figure 3 depicts some applications of digital image watermarks and Table 4 summarizes the basic requirements of watermarking schemes together with their related applications.

Any image watermarking scheme must fulfill these basic requirements (robustness, capacity, imperceptibility, and security) to be considered viable for practical applications. Thus, a watermarking scheme can be evaluated based on these requirements [54], [55]. The following subsections introduces the various applications of digital image watermarking that rely on these requirements.

A. COPYRIGHT PROTECTION

In this application, a robust watermark is embedded into the host image, which represents the ownership or copyright information. The copyright information that is embedded as a watermark allows owners of a digital image or other multimedia content to protect their rights and demonstrate their ownership in case of a dispute [56]. A robust watermark implies that it should be difficult for an adversary to remove or destroy the watermark from the watermarked object even at exceedingly severe conditions. Furthermore, a watermarked object should still be easily identified and the watermark should be seamlessly extracted even after it has been subjected to various removal attempts and brute distortion attacks. Notably, all geometrical or non-geometrical attacks that attempt to destroy and remove the robust watermark should cause substantial degradation to the visual resolution of the watermarked image. In contrast, the extracted watermark must have low distortion to facilitate identification of the host image's rightful owner.

B. AUTHENTICATION

Digital content can be easily tampered with while avoiding detection. Authentication and verification of the integrity of digital content must be performed to ensure that no unauthorized modifications are performed. It is imperative to ensure that the integrity of digital content remains intact as they are leveraged in sensitive applications such as legal cases, police investigations and medical use. Thus, various digital authentication techniques have been presented in the literature [8]. Cryptography-based measures have been widely explored to solve this problem using hash functions, message authentication code and digital signature.

In digital image authentication, cryptography hash functions and digital signature encryption method are adopted to preserve the integrity of data content. A hash value of

$$NC(W, W^{new}) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[W(i,j)-\mu_1][W^{new}(i,j)-\mu_2]}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[W(i,j)-\mu_1]^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[W^{new}(i,j)-\mu_2]^2}} \quad (3)$$

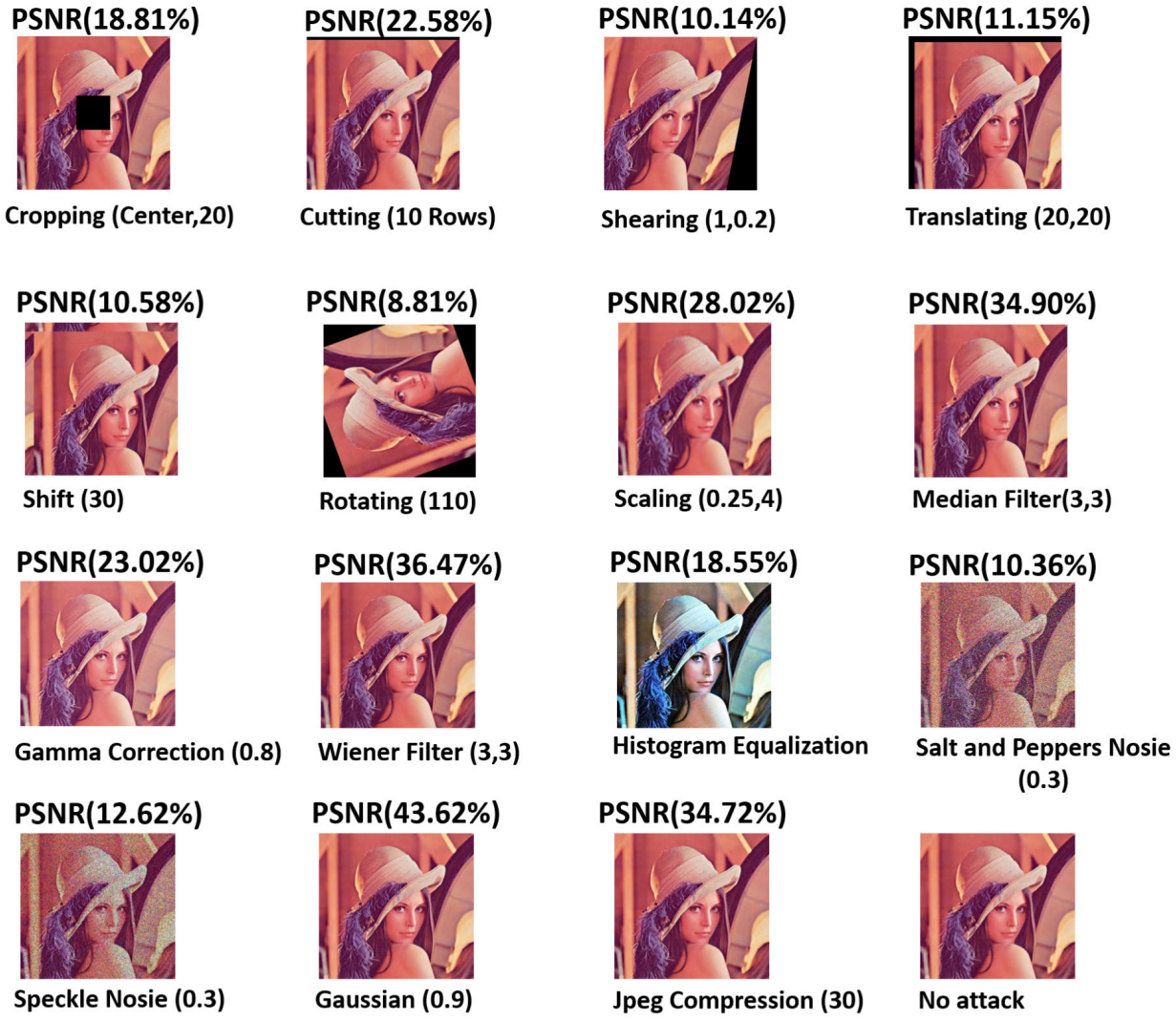

FIGURE 2. Attacks for robustness analysis.

the digital image is computed and then is used to generate a digital signature. To authenticate a received image, a new hash value is computed using the same hash function and compared with the one being stored. If the two hash values match then the digital image is regarded as been authentic. The advantage of cryptography-based image authentication techniques is that unauthorized parties are unable to create a new signature as long as they do not have the private key. However, the main problem of the cryptography-based image authentication techniques lies in the storing location that is used to save the signature. Consequently, it becomes difficult to verify the image authenticity if the storing location is removed or altered [57], [58].

On the other hand, image watermarking is an alternative technique used to achieve image authentication. To detect image tampering, watermarking-based image authentication techniques have been proposed based on fragile and semi-fragile watermarks [59]–[62]. By embedding a fragile watermark directly into the host image, any efforts to tamper the watermarked image will result in distortions to the extracted watermark. This allows quick detection of image integrity problems. Therefore, watermarking-based authentication is more advantageous as compared to cryptography-based authentication for two reasons. Firstly, it is difficult to remove the embedded watermark and tampering attempts it will

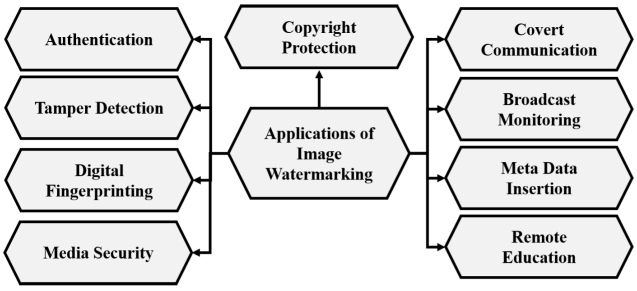

FIGURE 3. Application of digital watermarking [2].

TABLE 4. Requirements of digital image watermarking schemes and corresponding applications [2].

Basic Requirements	Definition	Applications
Robustness	To recovery and extract embedded watermark efficiently under various attacks	Copyright protection, Digital image processing, Graphics, telemedicine, and forensic applications.
Impressibility	It is focused on how can embed a watermark imperceptibly without distortion or degradation that appears on a watermarked image.	Digital Imaging, telemedicine, Digital Documents, Claim of ownership, Network patrolling, Meta level etc
Security	It is regarding that a watermark cannot be removed or altered without destroying the host image from unauthorized parties	Telemedicine, Fingerprinting Military
Data payload	This scale expresses the magnitude of data that can be embedded with achieving a trade-off between robustness and imperceptibility of the watermarked image.	Digital image Telemedicine
Capacity	This factor focuses on describing number of watermarks that can be embedded in a host image or other objects at the same time.	Telemedicine, Media distribution, Authentication

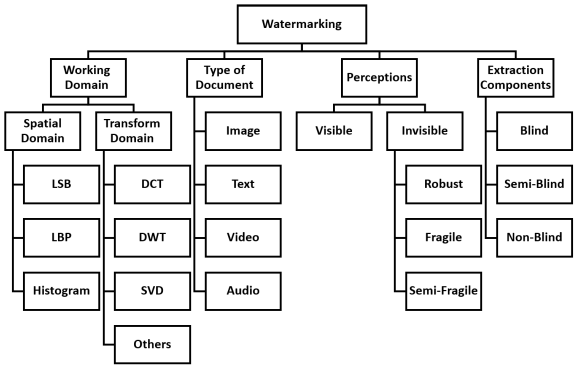

FIGURE 4. Classification of digital watermarking strategies.

lead to changes to the watermark itself. Secondly, the storing location is not used to save the watermark data. Semi-fragile watermarks that have low robustness are used to detect tamper locations, modifications, and manipulation of a watermarked image [63], [64]. These watermarks should be invisible and fragile at the same time. The difference between two types is based on the type of authentication. Fragile watermarking schemes are better suited for full authentication of digital images without any modification whereas semi-fragile watermarking schemes focus on content authentication while allowing some form of tampering to the digital image. Semi-fragile must also be robust to protect the content.

C. OTHER APPLICATIONS

Image watermarking has other applications such as broadcast monitoring, digital forensic, military, network flow watermarking, watermarking cloud computing, electronic voting and big data watermarking [39], [55]. Moreover, many other applications can be possibly included digital image watermarking framework. Table 5 details some of these image watermarking applications.

TABLE 5. Image watermarking applications.

Applications	Descriptions
Broadcast Monitoring	Helps owners monitor digital content that has been broadcast over different media such as terrestrial, cable, or satellite TV. Digital watermarking plays a major role in preserving intellectual property, traceability, and copy control.
E-Voting	An alternative to the conventional voting process that introduces the security mechanisms required for fraud prevention and voter privacy protection. Digital watermarking offers a valuable alternative by continuing to recognize the voters.
Digital Forensics	Image watermarking helps in acquisition, coding, and editing of digital traces or evidence.
Fingerprinting	The watermarked image contains the intended recipient's identification information to prevent or trace the source of unauthorized distribution.
Source Tracking	Convert a digital watermark into a binary stream that is embedded into a digital signal. The watermark can be retrieved from the distributed signals to identify or track the distribution source.

V. CLASSIFICATIONS OF DIGITAL WATERMARKING SCHEMES

Various digital watermarking schemes have been proposed for different purposes [7], and can be classified based on various criteria. We can classify them based on the extraction components, working domain, human perception and the type of document related to the host object, as shown in Figure 4. For types of documents, image, video, text, and audio are common ones. However, images have gained the most attention due to their abundance on the Internet, and the fact that digital images may contain sensitive information. As compared to text, the digital images are easily intercepted or obtained as they are usually transmitted or displayed openly. Therefore, image watermarking techniques are of great interest to researchers as there is a need to provide various protection mechanisms. In the following subsections, the three remaining classifications are detailed.

A. CLASSIFICATION BASED ON THE EXTRACTION COMPONENTS

A watermarking framework has two important processes namely embedding and extraction. The extraction process may require additional information such as the key (side information), the original watermark, and the original host image without a watermark. Watermarking schemes can be classified into three types based on the type of information required for extraction:

- **Blind** - A blind watermarking scheme only requires the watermarked image and a key for watermark extraction. The original watermark and host images are not required for extraction. A blind watermarking scheme is suitable for medical applications because original images containing patient information or diagnosis should not be made available [65], [66]. This type of scheme is

also referred to as an oblivious or public watermarking scheme.

- **Non-blind** - A non-blind watermarking scheme requires at least one additional component (original host or watermark image) apart from the watermarked image and key to recover the embedded watermark [67]. Non-blind watermarking schemes are used in a variety of applications such as copyright and identification of ownership [43], [68].
- **Semi-blind** - A semi-blind watermarking scheme is a subcategory of blind watermarking schemes. It uses a key and also the original watermark in the extraction process. The original host image is not required [69].

B. CLASSIFICATION BASED ON WORKING DOMAIN

Based on the working domain, watermarking schemes can be categorized into two main groups: spatial and transform (frequency), each having its own set of pros and cons. Existing image watermarking schemes based on the two domains are discussed in the following subsections.

1) SPATIAL DOMAIN METHODS

Usually, watermark data is embedded directly into the pixels of the host image. The least significant bit (LSB) is usually selected for embedding to maximize the quality of the watermarked image [41]. Spatial-based watermarking schemes have the advantage of being fast, simple, and can handle a large payload (large capacity for embedding watermarks). Furthermore, a small watermark can be embedded many times into the host image. In this case, the probability of destroying and removing the embedded watermarks by using well-known attacks is very low. If some of the watermarks are removed, at least one watermark that fulfills the purpose will still survive [61], [70].

However, spatial-based watermarking schemes have low resistance against non-geometric attacks such as noise and lossy compression. Moreover, most schemes that rely on the spatial domain involve some generic steps to complete the embedding process. When these steps are known, the watermark can be easily destroyed and modified by an adversary. Figure 5 shows the generic steps of a spatial-based image watermarking schemes. Firstly, the host image and watermark are converted into binary values (8-bit values). This is referred to as the binary process. Secondly, the LSB of each 8-bit value of the host image is replaced by bits taken from the watermark. Finally, the altered values are converted back into pixels to form the watermarked image [71], [72].

Local binary pattern (LBP) is another technique that differs from the general method [62], [73], [74]. LBP has been successfully applied in various domains such as face recognition, texture analysis, and crowd estimation [75]–[77]. In LBP, the host image and the watermark is divided into non-overlapping blocks, then the contrast of each block is calculated. Pixels obtained for embedding and extracting is based on LBP, which calculates the spatial relationship between the central pixel and its adjacent pixels in each block, as illustrated in [61]. LBP-based watermarking methods have some merits that make them better than LSB-based methods such as resistance to some attacks, contrast adjustment, and luminance change. LBP is also considered a fragile watermark, thus a LBP-based method is considered a semi-fragile watermarking approach [41], [61].

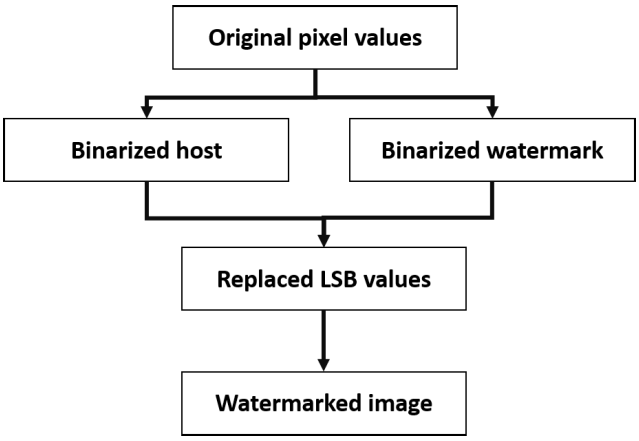

FIGURE 5. The general steps of spatial watermarking scheme.

Another method that uses the spatial domain is referred to as histogram modification [78]–[80]. It focuses on collecting the common features of the host image to be used in the embedding process. The main notion behind this method is shifting values of histogram intensity between the minimum and the maximum bins for hiding data. This is achieved by modifying pixel values. It is easy to implement and minimal side information is needed for extraction. However, the payload is limited because there is only a small difference between the maximum and minimum bins [81].

2) TRANSFORM DOMAIN METHODS

To generate frequency coefficients, several transformation methods have been developed for different applications such as watermarking, signal processing and data compression. For image watermarking schemes based on the transform domain, a transformation is implemented onto the host image to generate frequency coefficients. The next step modifies the frequency coefficients of the host image by embedding the watermark information. Finally, the watermarked image is obtained after performing an inverse transform. A small modification of the frequency coefficients is less likely to be detected by human visual systems (HVS). Many transformations are used in image watermarking designs such as discrete Fourier transform (DFT),discrete cosine transform (DCT), discrete wavelet transform (DWT), dual-tree complex wavelet transform (DTCWT), contourlet transform, or SVD. Table 6 provides a comparison between these approaches. The transform domain in the watermarking designs has some advantages over the spatial domain such as robustness against geometrical and non-geometrical attacks and frequency coefficients that HVS are less sensitive to.

TABLE 6. Comparison between spatial and transform domain in watermarking methods.

Criteria	Transform domain watermarking	Spatial domain watermarking
Definition	Transform to frequency coefficients and change these them.	Using LSB of image pixels and embedding directly into pixels.
Capacity	The maximum embedding is the same size of sub band.	The maximum embedding is the same size of the host image.
Robustness	High probability of extracting a watermark under different attacks	Low probability of extracting a watermark under different attacks
Imperceptibility	Hard to find a watermark.	Easy to find a watermark.
computational complexity	High	Low

1-Discrete Cosine Transform (DCT)
DCT is widely used in watermarking methods, which has good energy compaction properties. After application of DCT, the image energy is distributed into low, high and middle-frequency coefficients [82], [83]. The middle frequency is always selected to embed watermark information to achieve the trade-off between robustness and imperceptibility.

Three parts of a matrix can be created by applying DCT. F_L denotes the lowest energy of frequency coefficients of the block, whereby F_H denotes the higher energy of frequency coefficients. F_M is used to denote the middle region that is chosen for the embedding process because of noise and attack resistance, and preventing major alterations. DCT can be mathematically calculated for a one-dimensional data series and two-dimensional data matrix. For an image I of size $M \times N$, DCT coefficients (D) can be obtained from the transformed image using Eq. 4. $I(x, y)$ is an input image and x denotes to row, while y denotes to column. $D(i, j)$ is DCT coefficients where i and j denote the row and column of the DCT matrix [84].

$$D(i,j) = \frac{2}{\sqrt{MN}} C(i)C(j) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} I(x,y) \cos\frac{(2x+1)i\pi}{2M} \cos\frac{(2y+1)j\pi}{2N}. \quad (4)$$

where

$$C(i)C(j) = \frac{1}{\sqrt{2}} \text{ if } i \text{ and } j = 0, \text{ elsewhere } C(i)C(j) = 1. \quad (5)$$

A considerable amount of literature on watermarking schemes based on DCT has been published. Several studies have highlighted how DCT techniques are robust against different attacks [51], [85]–[89]. Ali *et al.* proposed an algorithm to achieve a trade-off between robustness and imperceptibility [51]. The host image is split into non-overlapping blocks and the DCT domain transforms each block. The collected DC coefficients for each block are constructed using a new low-resolution image and SVD is applied to embed the watermark by altering the singular values S of the SVD coefficients.

Parah *et al.* proposed a new DCT watermarking scheme by dividing the host image into blocks and the DCT is applied to each block [86]. The difference between two adjacent blocks of DCT coefficients is then calculated. Using watermark bits and some predefined conditions, the middle-frequency coefficients are modified for one of the two blocks to highlight the difference in a specified range. The inverse transform is applied to obtain the watermarked image. The difference range is used in the extraction process. Liu *et al.* have developed a watermarking scheme based on fractal encoding and DCT [87]. Fractal encoding and the DCT have been combined in a dual encryption processes to develop the classical DCT technique.

Alotaibi and Elrefaei have proposed a text-image watermarking scheme based on hybrid integer wavelet transform (IWT) and DCT [88]. IWT is first applied to the host image and the LL sub-band is selected to apply the DCT domain. The medium DCT frequency coefficients are chosen to embed a watermark. Wu and Sun have proposed a robust copyright scheme based on DCT and SVD [89]. A host image is divided into overlapping blocks and DCT is applied. DC values of each block are collected to construct a new DC-map. SVD is then applied and a master share generated. A secret share and master share are used to build the ownership share. Lossless and blindness are fulfilled in this scheme and it is resistant to different well-known attacks.

Other watermarking schemes have been proposed based on hybrid DCT with other transforms such as DWT+DCT+SVD [19], [25], SVD+DCT [90], quaternion (QDCT)+ SVD [22], DCT+DWT [91]–[93]. However, the major drawback of DCT-based schemes is that the host image is deformed in a non-reversible way so that it cannot be restored accurately [41].

2-Discrete Wavelet Transform (DWT) DWT is widely used in many signal processing applications. It is a mathematical tool based on time, and has been used in transient analysis and time-varying on the signals. Since real-life signals always change over time, wavelet transformation is more

suitable for a number of applications such as image denoising, data compression, and fingerprint verification [94]. Wavelet transform is efficient for image processing because it has the ability to highlight local and global image characteristics. In image processing, DWT can be applied to an image and produce a frequency coefficient and a spatial description. DWT processes are achieved by passing an image through a series of high-pass and low-pass filters to produce high and low frequency. Thus, DWT decomposes the image into a set of four sub-bands with different frequencies.

The four non-overlapping sub-bands, approximation image (low frequency)(LL), horizontal (HL), vertical (LH) and diagonal (HH) components have different resolutions. LL has lower resolution approximation as compared to HL, LH and HH. LL provides a rough illustration of an image by passing it through a low-pass filter in both directions to obtain the LL sub-band. Whereas to obtain the LH and HL sub-bands, the image is passed through a low-pass and high-pass filters. The image is passed through the low-pass followed by high-pass filter to obtain the LH sub-band and vice versa to obtain the HL sub-band. An image is passed through a high-pass filter in both directions to obtain the HH sub-band. The HH sub-band has high-frequency elements along its diagonal values. LL sub-band holds most of the information of the original image whereas the LH and HL sub-bands hold the detail information of the horizontal and vertical edges, respectively. Therefore, LL sub-band is used in the embedding process to achieve the good balance between watermarking requirements.

The decomposition process can then be repeated for each sub-band to obtain multiple-scale resolutions. The size of each sub-band is a quarter of the original image in the first decomposition, and the size of the sub-bands can be further reduced if need. The main advantage of DWT over DCT transform is that an update of the sub-band frequency coefficients will have an impact on the entire image unlike DCT which has a local impact.

The LL sub-band has low pass features, and embedding a watermark in this sub-band leads to high resistance to various attacks such as loss of compression, distortion, and geometric distortions. However, it is susceptible to other attacks that can distort the embedded watermark such as histogram equalization, gamma correction, and contrast adjustment [95]. Instead, embedding a watermark in the detail sub-bands (LH, HL, and HH) will reduce the vulnerability of the watermarked image to modifications that can be detected by HVS, thus attaining elevated imperceptibility. This is as a result of the detailed sub-bands having an elevated frequency, to which human vision is less sensitive to [96].

Based on a review of various DWT-based watermarking schemes, we found that DWT has been applied to improve robustness. In DWT schemes, the host image is usually decomposed either into 1-level [97], [98] or multiple levels [99], [100]. Gao *et al.* applied a 2-levels DWT onto a host color image [101] whereas the grayscale watermark image is scramble by Arnold transform. The scrambled watermark is embedded into the LL sub-band of the blue and green channels.

Giri *et al.* used DWT to decompose the host image, where 1-level of the HL sub-band is selected to embed the watermark [102]. Cupta *et al.* decomposed the host color image into 3-levels resolution sub-bands [103], the all 3-levels sub-bands of all channels are selected to embed the watermark. ABC and uncorrelated color space are used as a trade-off between imperceptibility and robustness. Huynh *et al.* proposed a watermarking scheme based on DWT and difference quantization algorithm [104]. DWT is applied to the host color image and the middle frequency (LH and HL) are chosen to embed bit watermark.

Hybrid watermarking schemes based on DWT and other transforms have also been proposed. Rasti *et al.* used DWT, SVD, orthogonal-triangular decomposition and chirp z-transform to embed the watermark [105]. DWT is applied in 2-levels, and LL sub-band is selected to embed singular values of the watermark. Roy *et al.* used DWT and SVD to propose a new watermarking scheme based on YCbCr color space [106]. Cb component is selected and decomposed into 4-levels sub-bands. The HL sub-band is selected to embed the singular values of the watermark.

Lakrissi *et al.* proposed a dynamic image watermarking scheme [107], 3-levels of DWT is applied to the luminance component of the host image, and the LL sub-band is divided into a number of blocks. Using a pseudo-random generator, a dynamic block is chosen randomly for the embedding process. In addition, other hybrid schemes based on DWT and other transforms have been proposed such as DWT+SVD [108], [109],DCT+DWT [91], [92], DWT+DCT+SVD [19], [25], and others [12], [110]

3-Lifting wavelet transform (LWT) LWT is a signal processing tool used in many applications such as image processing and compressing. One of the important properties of LWT is that it supports either floating-point numbers or integers unlike classical transforms that deal exclusively with floating-point values. The use of floating-point representation in image processing may result in loss of information due to round-off operations. As such, LWT is suitable for image processing because 8-bit integers are used to represent pixels.

4-Integer Wavelet Transform (IWT) IWT is a lifting transform that maps input data to integers without quantization errors and it is also reversible. It consists of three processes which are split, predict and update. Although it has similar processes to LWT, IWT is more computationally efficient. Figure 6 shows 1-level IWT of the Lena image, where four sub-bands are generated.

Fan *et al.* used Haar IWT with Harris corner detection to extract image features which is then used in the construction of a binary feature map [111]. Arsalan *et al.* used IWT domain to decompose a host image and a compression function in the embedding process to reduce distortion [50]. Shi and Lv proposed a watermarking scheme based on IWT, where the watermark is embedded into the LL_5 sub-band [66]. Makbol and Khoo proposed a watermarking scheme to solve the FPP

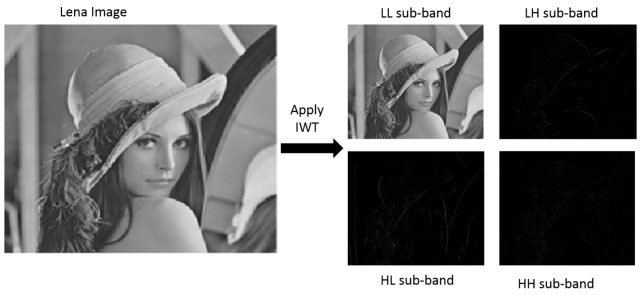

FIGURE 6. IWT sub-bands of Lena.

[112]. They used IWT and SVD to embed a watermark and generate a signature from two singular vectors of the embedded image. The signature is obtained before the watermark is processed in the extraction phase.

In a separate scheme, Makbol and Khoo applied IWT to the host image, followed by SVD on all sub-bands [113]. An Arnold transform is also included to scramble the watermark for increased security. Then, the scrambled watermark is directly embedded into the singular values of the host image. Alotaibi and Elrefaei proposed a text-image watermarking scheme hybridizing IWT and DCT [88]. Wang proposed a novel combination of image encryption and watermarking [114]. In the embedding phase, a reversible IWT and histogram modification is used. Lossless watermark information is embedded in the encrypted host image by inverse IWT.

In another scheme, Makbol *et al.* decomposed the host image using IWT and selected the LL sub-band for embedding [24]. SVD is applied to the LL sub-band and the watermark image. The singular vectors, U of the watermark image are embedded into singular values S of the host image's LL sub-band. The multi-objective ant colony optimization (MOACO) is used to select a multi-scale factor to achieve a good trade-off between imperceptibility and robustness.

5-Singular-value decomposition (SVD) SVD is a numerical tool that decomposes any matrix into three matrices or vectors. An image, I can be considered matrix which consists of 8-bit numbers with a variety of dimensions depending on the type of image. For example, a grayscale image has a dimension of $1\times N\times N$ whereas a color image has a dimension of $3\times N\times N$, where N is the size of the matrix. An image can also be denoted as a matrix I of real numbers $\mathbb{R}^2$. SVD can be applied to I, resulting in three matrices, U, S, and V. Anyone can recover the original matrix with knowledge of these three matrices. SVD of I with rank r, $I(r \leqslant N)$ can be defined as [18], [47], [115]

$$SVD(I) = U_I S_I V_I{}^T = \sum_{i=1}^{r} U_I * S_I * V_I{}^T. \tag{6}$$

$$U_I = [u_1, u_2, \ldots, u_N] \tag{7}$$

$$V_I = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_N \end{bmatrix} \tag{8}$$

$$S_I = \begin{bmatrix} s_1 & 0 & \cdots & 0 \\ 0 & s_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & S_N \end{bmatrix} \tag{9}$$

where U_I and V_I are orthogonal matrices of $\mathbb{R}^{N\times N}$. These matrices, which will be henceforth referred to as the left and right singular vectors of matrix I (eigenvector), are highly sensitive to changes in the original matrix, I. S_I is a diagonal matrix of $\mathbb{R}^{N\times N}$ that consists of positive singular values in descending order as $s_1 \geqslant s_2 \geqslant \ldots \geqslant s_N$. T denotes the conjugate transpose operation. Researchers leverage upon the following properties of SVD in designing image watermarking schemes:

- The diagonal values in S are highly stable. When there are small changes to these singular values, there will be barely any effect on the resulting image pixels. Thus, watermark information can be embedded without affecting the visual perception of the host image.
- Due to how the singular values in S are in descending order, the smaller values are located towards the end of the matrix. Adding or updating these smaller values during the recovery stage has minimal effect on image quality. In addition, adding new small values in all positions in S also has minimal effect on image quality.
- U_I and V_I hold the geometry characteristics of the image and S_I represents the luminance of the image.
- SVD can be applied to different image sizes.
- S_I values can resist geometric distortions such as transpose, rotation, scaling, translation, and Flip. Singular values remain non-zero after these distortions, which do not affect the alteration.

Recently, SVD has been used alongside other frequency transforms in image watermarking schemes [19], [24], [25], [116]. In the following sections, the hybrid image watermarking schemes based on SVD and other transforms will be introduced in detail.

C. CLASSIFICATION BASED ON HUMAN PERCEPTION

Digital watermarks can either be visible or invisible depending on the purpose of the watermark. Visible watermarks are embedded into the host image in a way that is visible to all viewers. This type of watermarking technique is mostly used in commercials to identify the owner of a product that is being sold. A watermark may be used as a logo containing extra information about the company or type of product. The main aim of visible image watermarking is to prevent illegal business use of media. It is simple to embed a visible watermark into an image but is difficult to remove [48].

As for invisible watermarks, a watermark is embedded into the host image in a manner that is imperceptible or hard to

detect. Invisible watermarks need to be embedded algorithmically whereas visible watermarks may be embedded manually. There are four types of application-specific invisible watermarking schemes [117] which are:

- **Robust watermarking** - For copyright protection and proof of ownership, a watermark should be difficult to destroy or be detected by unauthorized parties. Robust watermarking uses different methods to embed watermarks to ensure high robustness. The embedded watermark should withstand various geometric and non-geometric attacks, preventing degradation and tampering or elimination of the watermark.
- **Fragile watermarking** embeds a watermark that is easily destroyed or altered by minor modifications. Fragile watermarking schemes are suitable for authentication and integrity applications.
- **Semi-fragile watermarking** allows an embedded watermark to be modified to a certain extent but the watermark can still be easily destroyed by malicious attacks. This type is usually used in special cases requiring authentication and tamper detection. For example, lossy image compression is considered an acceptable modification because it is used to reduce image storage requirements whereas geometric attacks are considered to be targeted or malicious attacks.
- **Hybrid watermarking** is a combination of fragile and robust methods for providing copyright protection, authentication and integrity simultaneously [118].

VI. HYBRID SVD-BASED IMAGE WATERMARKING SCHEMES

In this section, SVD and other frequency transforms (hybrid schemes) are reviewed. Many hybrid SVD watermarking schemes have been designed for the purpose of copyright protection. The popularity of SVD is due to the stability of the singular values in the S matrix, whereby small changes do not affect the visual perception of the host image. In addition, SVD has a low computational complexity when applied to a sub-band of the host image. Although most hybrid image watermarking schemes have shown to be robust, they have not been able to address some security issues such as FPP, false-negative errors and message errors [47]. FPP is one of the key issues that needs to be taken into account as false watermarks can be generated or detected from an image that contains the original watermark [18].

Let H and W denote the host image and watermark image respectively. First, H and W can be converted into the frequency by using one of the various transform methods. Based on Eq. 10 [115], [119], W can be added to one of the SVD components, S. SVD is performed on the host image. Then W is embedded in S based on a scaling factor, α which controls imperceptibility and robustness. $S_{new} = S+\alpha \times W$ is a formal equation commonly used in SVD watermarking schemes. Next, the new singular values S_{new} is used instead of S in an inverse SVD operation to obtain the watermarked image H_W. PSNR should be high in order to achieve low distortion in the watermarked image [115], [119].

$$\begin{aligned} H &\overset{SVD}{\Rightarrow} USV^T \\ S_{new} &= S + (\alpha \times W) \\ H_W &\overset{SVD}{\Leftarrow} US_{new}V^T \end{aligned} \tag{10}$$

During extraction, the two components of the watermark S_{new} and α are kept and used as the key (side information). To extract watermark information from a watermarked image ${H^*}_W$, the SVD steps in Eq. 11 is performed in reverse. The extracted watermark can be described as follows [115], [119]:

$$\begin{aligned} H_W &\overset{SVD}{\Rightarrow} U_W S_W {V^T}_W \\ W^* &= \frac{1}{\alpha}(S_{new} - S_W) \end{aligned} \tag{11}$$

During the detection process, the effect of different geometric and non-geometric attacks on NC values are investigated. The NC values should be close to ideal value to indicate that a particular scheme is robust. There are seven general embedding methods used for SVD-based watermarking image schemes found in the literature. These embedding methods and their descriptions are presented in Tables 7 and 8. The first method involves embedding the singular value of watermark in the singular value of the host image, which we refer to as singular value matrix watermarking (SVMW). The second method involves embedding a watermark directly in the singular values of the host image which we refer to as direct watermarking (DW). The fifth method involves comparing the middle singular value of watermark with corresponded in the host image and then embedding, which we denote as singular value and comparison (SVC) methods. These three are affected by FPP because they use singular values for embedding.

on the other side, the third method, comparison and threshold (CT) uses binary watermark image with threshold value to change U of the host image. The fourth method based on principle components (PC) uses US of the watermark image to embed into the host image. Singular Vectors (U or V) methods use one of the singular vectors to embed in the host image, CT, PC, and Singular Vectors (U or V) can overcome FPP. Furthermore, CT and SVC methods have low embedding capacity due to having only one or two changes in the singular value or singular vector values. Zero methods are used in several schemes, which involve extracting the master share that will be further XOR-ed with the watermark image.

A. SVD-BASED IMAGE WATERMARKING CLASSIFICATION

SVD-based image watermarking schemes can be divided into several classes as shown in Figure 7. With regards to the embedding process, there are six types of techniques that can be used based on SVD components. These embedding methods include singular values [120], left singular vectors [24], [27], [121], right singular vectors [122], PCs [123], [124], left and right singular vectors [125], and zero embedding watermarking schemes [46], [126]–[128]. All these methods

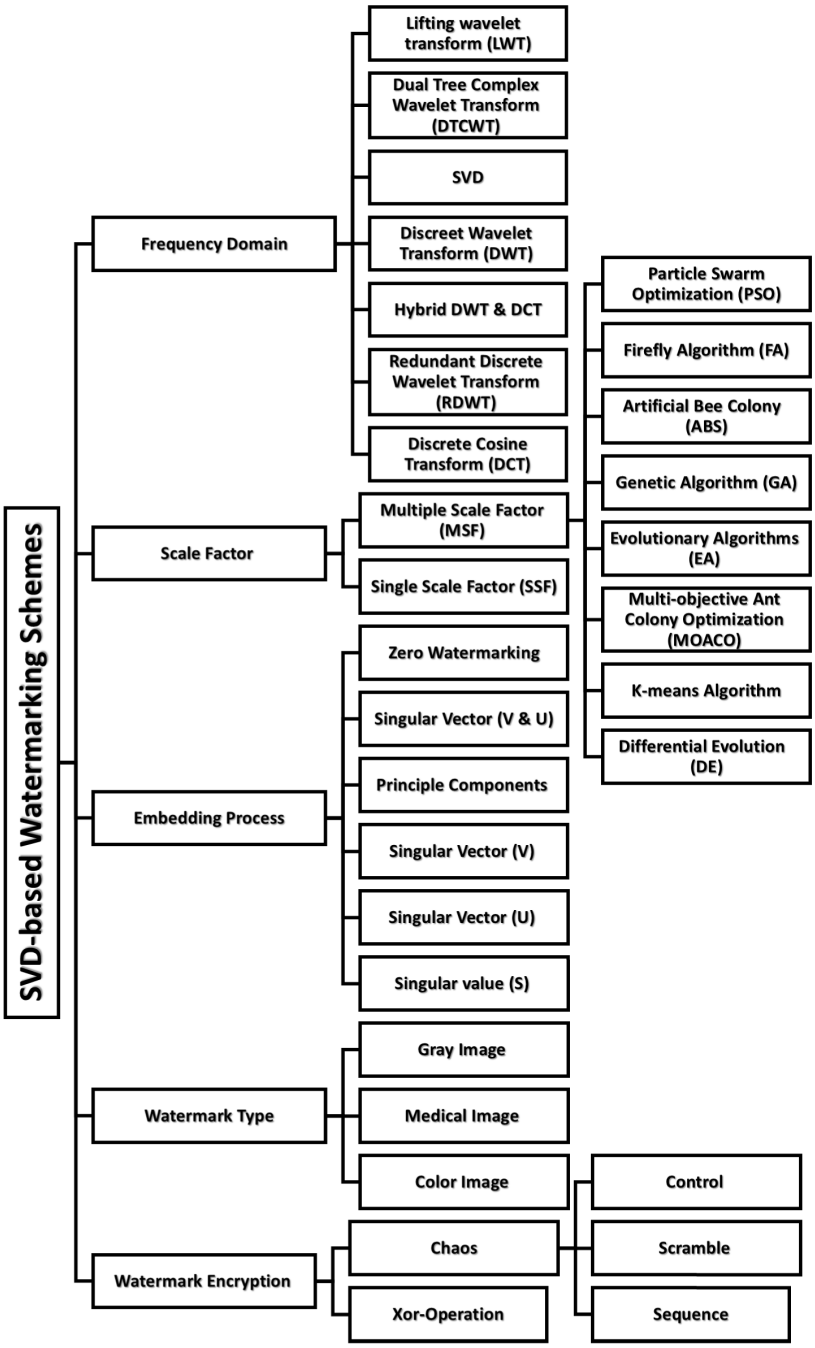

FIGURE 7. SVD-based image watermarking classification.

except zero watermarking embed watermark information into one or two of the SVD components.

For schemes in the frequency domain, the host image is converted into frequency bands. Different techniques are used to transform from spatial domain to frequency domain such as DCT, DWT, redundant discrete wavelet transform (RDWT), LWT, DTCWT and DCT+DWT. Here, SVD is applied to the frequency coefficients, then watermark information is embedded by altering the SVD component coefficients.

SVD watermarking schemes can also be classified based on watermark type. Gray or grayscale images are used in many watermarking schemes, whereby small dimensions of 32 $\times$ 32 pixels are popular [84], [129], [130]. The techniques mentioned earlier are used to achieve a good trade-off between robustness and imperceptibility. Having

a smaller dimension (smaller payload or capacity requirements) reduces the distortion of the watermarked image and improves resistance to different attacks. Colored watermarks are another popular type which consists of three channels that are each embedded in the host image, implying the need for a scheme with higher capacity [12], [121], [131]. This type of image watermark still needs further study because colored images are large payloads that can lead to significant distortion of the watermarked image [44], [132]. The CT type of watermark are medical images that can be divided into two types, namely patient information and logo of hospital or clinic [19], [133]. Medical images could be considered a sub-type of gray or colored images. Host images themselves are usually patient-related medical images.

SVD-based watermarking schemes can also be classified based on their scale factor. Scale factor plays an important role in image watermarking because it determines the embedding trade-offs. A single scaling factor (SSF) can lead to a stable level of embedding, but it cannot fulfill the desired balance between robustness and imperceptibility. For example, a small SSF value can lead to high imperceptibility but lower robustness against common attacks. On the other hand, a large SSF value improves robustness while sacrificing imperceptibility. Thus, researchers have used multiple scaling factors (MSF) instead of SSF to achieve the desired goals of robustness and imperceptibility.

Optimal MSF values can be determined by using optimization algorithms such as GA [134], particle swarm optimization (PSO) [135], MOACO [24] and differential evolution (DE) [45], [51], [126]. MSF-based optimization techniques achieve all requirements of a good image watermarking scheme. However, the use of optimization techniques are computationally expensive, and there is a limited range of suitable MSF values for each watermarking scheme.

Collectively, watermark security is very important and is a key technology for copyright protection. In recent years, various techniques have been used to encrypt watermark information before its embedding into the host image. Thus, we can also classify watermarking schemes based on the use of encryption methods, which include XOR-based encryption or chaos-based encryption. Watermarks can be encrypted via bit-wise exclusive OR (XOR) with random sequences, similar to how stream ciphers operate [136]–[138]. On the other hand, chaos-based watermark encryption has been used in many schemes to improve security [17]. The use of digital chaos in image watermarking can be further divided into three classes:

1) Chaos-based scrambling - Chaotic systems such are used to scramble positions of pixels of the watermark image, such as Arnold map [139], [140] and logistic map [84], [133]. Arnold transform is a two-dimensional chaotic map used in many watermarking schemes to permute image watermark pixels because it is a one-to-one mapping. The logistic map is a simple one-dimensional chaotic map that can be used in the two ways: first is to permute image pixels by sorting them based on a data sequence generated by the map, and the second is to generate a key-stream for encryption (XOR).
2) Chaos-based control of the embedding position - A chaotic sequence is used to control the selection of blocks from the host image for embedding purposes [141], [142].
3) Chaos-based sequence - Chaotic sequence is used directly in the embedding process instead of the watermark image [143].

B. FALSE POSITIVE PROBLEM (FPP) ATTACKS AND SOLUTIONS

There are two main embedding algorithms that are used in the design of SVD-based watermarking schemes that lead to FPP. The first embedding algorithm (SVMW) uses the singular values of the watermark to be embedded in the singular values of the host image. The DW embedding algorithm uses watermark information to be embedded directly into the singular values of the host image. The SVMW method can be defined as [115], [144]

$$S_{New} = S_H + \alpha \cdot S_W \tag{12}$$

where S_{New} denotes the singular values of the host image after modification, α is the scaling factor, S_H and S_W represent the singular value matrices of host and watermark image respectively.

Figure 8 depicts the SVMW embedding algorithm based on Eq. (12) that leads to FPP [24], [29], [145], [146]. The watermark and host image are decomposed using SVD, then S_H and S_W are used with the scaling factor to generate S_{New}. S_{New}, U_W and V_W are used as side information or keys in the extraction algorithms [29], [125], [135], [147]. An adversary can use side information for any watermark, extract the singular values, S and then claim ownership for the watermark. This is because S does not have geometrical content for digital images.

In the DW type, the watermark is embedded directly into the host image, which leads to FPP vulnerability. It can be expressed as [144]

$$S_H + \alpha \cdot W = U_{HNew} S_{HNew} V^T{}_{HNew} \tag{13}$$

where W is the watermark information, U_{HNew}, S_{HNew}, and $V^T{}_{HNew}$ are three matrices obtained by applying SVD to the result of the embedding operation. This is a popular approach where the watermark is more visible, and the scheme is more robust [65]. The host image is decomposed by SVD and its singular value, S_H is modified by the scaling factor α multiplied by the watermark itself W. Then, the modified singular values are decomposed into three matrices by SVD. The new singular value matrices are used as side information or keys [29], [51], [65], [112], [113], [126], [145].

Both SVD-based embedding approaches are susceptible to FPP due to the following properties:

- The singular value, S of the image does not contain significant information about the structure of the image.

TABLE 7. SVD embedding common methods based on the literature review.

Embedding method	Embedding (Mathmatically)	Details	Key or side information	Extracting (Mathematically)	Details
SVMW	1- SVD $\Rightarrow W = U_w S_w V_w$ 2-SVD $\Rightarrow H = U_h S_h V_h$ 3-$S_{new} = S_h + (S_w \times \alpha)$ 4-$H_w = U_h S_{new} V^T$ iSVD	1-SVD is applied to the watermark W. 2-SVD is applied to the host image H. 3- Generating a new matrix S_{new} through multiply scale factor α with singular values of watermark S_w and adding to singular values of the host image S_H. 4-The new matrix S_{new} is used instead of S_H in the inverse SVD of the host image to generate the watermarked image.	U_w, V_w,α and S_{new}.	1- SVD $\Rightarrow H_w = U_h S_{hw} V_h$ 2-$S_w = (S_{new} - S_{hw})/\alpha$ 3-$W_{Extracted} = U_w S_w U^T{}_w$ iSVD	1-SVD is applied to the watermarked image to obtain S_{hw} 2- Form key, the S_{new} and α are used to get S_w 3-Inverse SVD by using scalar vectors and new matrix S_w to get the watermark.
DW	1-SVD $\Rightarrow H = U_h S_h V^T{}_h$ 2-$S_{new} = S_h + (W \times \alpha)$ 3-SVD $\Rightarrow S_{new} = U_{wh} S_{wh} V^T{}_{wh}$ 4-$H_w = U_h S_{wh} V^T{}_h$iSVD	1- SVD is applied to the host image H 2-Using the watermark matrix directly to generate a new matrix $S_{new}$with help scale factor and original singular value. 3- SVD is applied again on the new matrix S_{new} to generate three components. 4-The new singular values S_{wh} is used in inverse SVD to obtain a watermarked image.	U_{wh}, V_{wh} ,α and S_h.	1- SVD $\Rightarrow H_w = U_{hw} S_{hws} V_{hw}$ 2-$S_d = U_{wh} S_{hws} V_{wh}$ iSVD 3-$W^* = (S_d - S_h)/\alpha$	1-SVD is applied to the distorted watermarked image to obtain S_{hws}. 2-Using the singular vectors U_{wh} and V_{wh} from key and inverse SVD is applied to obtain S_d. 3-Using the α and S_h from the key with S_d, the watermark is extracted.
CT	1-if $W_{bit} = 1$ then $U(2,1) = sign(U(2,1)) \times (U_{avg} + \frac{T}{2})$ $U(3,1) = sign(U(3,1)) \times (U_{avg} - \frac{T}{2})$ $\lvert(U(2,1) - U(3,1))\rvert > Tand(U(2,1)(3,1))$ 2-if $W_{bit} = 0$ then $U(2,1) = sign(U(2,1)) \times (U_{avg} - \frac{T}{2})$ $U(3,1) = sign(U(3,1)) \times (U_{avg} + \frac{T}{2})$ $\lvert(U(2,1) - U(3,1))\rvert > Tand(U(2,1) < U(3,1))$	1- The host image is divided to a set of blocks and SVD is applied for each block, the watermark converts to binary series. Based on the value of the binary digit 1 or zero, the U in the second row and third row of the first column are changed. If $W = 1$ the U(2,1) is larger than U(3,1) and the difference between them larger than the threshold value T. 2-If $W = 0$, then the $U(3,1)$ is larger than $U(2,1)$ and the difference between them larger than the threshold value T. U_{avg} is the average of U values in the block.	V_{wh} and S_h.	1-if$(U(2,1) > U(3,1)$ then $W = 1$ 2-if $(U(2,1)(3,1)$ then $W = 0$	The watermarked image is divided into a set of blocks and SVD is applied for each block. Check the $U(2,1)$ and $U(3,1)$ to find the binary watermark values. if $U(2,1) > U(3,1)$ then watermark binary is 1 and otherwise is 0.

TABLE 8. SVD embedding common methods based on the literature review.

Embedding method	Embedding (Mathmatically)	Details	Key or side information	Extracting (Mathematically)	Details
PC	1-SVD $\Rightarrow W = U_w S_w V_w$ 2-SVD $\Rightarrow H = U_h S_h V_h$ 3-$PC = U_w \times S_w, S_{new} = S_h + (\alpha \times PC)$ 4-$H_w = U_h S_{new} V^T{}_h$ iSVD	1-SVD is applied to the watermark and host image. 2- A PCs are calculated by multiplying U_w and S_w. 3- Inverse SVD is applied after substitution S_h of S_{new}	V_w, α and H.	1-$H_1 = H_w - H$ 2-$AW^* = \frac{1}{\alpha}(U^{-1} \times V^{T^{-1}})$ 3-$W^* = AW^* \times V^T$	1- Subtracting the host image form a distorted watermarked image to obtain a new matrix. 2- A PCs are obtained by α and inverse singular vectors. 3- Recover the watermark with multiplying PCs with V_w
SVC	1- for$i = 1 : B_L$ SVD $\Rightarrow B(i) = U_h S_h V_h$ SVD $\Rightarrow W(i) = U_w S_w V_w$ $S_h(n)^* = S_w(n)/\alpha$ 2- if $S_h(n) * > S_h(n)$ $S_h(n) = S_h(n)^*$ elseif $S_h(n)^* < S_h(n)$ $S_h(n) = S_h(n)$ 3-$B(i) = U_h S_h V^T{}_h$ iSVD	1- The host image and watermark image are divided into a set of non-overlapping blocks and SVD is applied to each block. L is a number of blocks and n is one of the middle singular values. $S_h(n)^*$ equals the middle of the singular values of watermark for each block divided by the scale factor. 2- Based on the condition, the middle value of the singular values of the host image is modified. 3-Inverse SVD is applied based on modified singular values.	U_w, V_w, and α	1-for $i = 1 : B_L$ SVD $\Rightarrow B^w{}_h(i) = U^w{}_h S^w{}_h V^w{}_h$ 2-$S_w(n)^* = S^w{}_h(n) \times \alpha$ 3-$W(i) = U_h S_h V^T{}_h$ iSVD	1-Divide the watermarked image into a set of blocks 2- SVD is applied to each block and the middle the singular values are taken to compute the singular values of the watermark image. 3-Inverse SVD of three components for each block to obtain extracted watermark image.
Zero	1-SVD $\Rightarrow H = U_h S_h V_h$ 2- If $S_h \geqslant S_{av}$ then $B_{i,j} = 0$, otherwise, $B_{i,j} = 1$ 3-$O = B_{i,j}$ xor $W_{i,j}$	1- The host image is converted by one of frequency transform. 2- One of sub band is selected to apply SVD. 3- The singular value or Singular vector is used to generate master share by using average value. 4- The binary watermark is xored with master share to generate owner share.	Owner share O	1-SVD $\Rightarrow H = U_h S_h V_h$ 2- If $S_h \geqslant S_{av}$ then $B_{i,j} = 0$, otherwise, $W_{i,j} = 1$ 3-$W_{i,j} = B_{i,j}$ xor $W_{i,l}$	1- The watermarked image is transformed by one of frequency transform. 2- The master share is generated based on SVD. 3- The binary watermark is extracted by xoring master share with owner share.
Singular Vectors (U or V)	1-SVD $\Rightarrow W = U_w S_w V_w$ 2-SVD $\Rightarrow H = U_h S_h V_h$ 3-$X = U$ or $X = V$ 4- $S_{new} = S_h + (\alpha \times X)$ 4-$H_w = U_h S_{new} V^T{}_h$ iSVD	1- The SVD is applied to the host image and watermark image. 2- the singular vector U or V is selected of the watermark image. 3- the embedding is performed based on scale factor and embed in singular values of the host image.	S_w, S_{new}, U_w or V_w, α	1- SVD $\Rightarrow H_w = U_{hw} S_{hws} V_{hw}$ 2-$X^* = (S_{new} - S_h)/\alpha$ 3-$W = XS_h V_w$ iSVD or $W = u_w S_h X$ iSVD	1- The SVD is applied to the host image. 2- the singular vector U or V is extracted from the watermarked image based on scale factor. 3- the inverse SVD is performed and the extracted watermark is obtained.

It does not express general aspects of the image content as it is merely the luminance of an image.

- The singular vectors, U and V contain information about image structure and have a strong effect on image content.
- If the singular values S is modified entirely, the contents of the image will not change.

Based on the highlighted reasons, the main challenge is in using U and V as keys for the extracting phase. SVD decomposes the watermark and the singular vectors, U and V are kept to recalculate the watermark during the extraction phase. An adversary may use his/her singular vectors (forged U_A and V_A) with the valid singular values, S_{HW} to extract a fake watermark from the watermarked image and claim ownership. This ultimately leads to three types of attacks which are [144], [148]:

- **Extracting Fake Watermarks**
  In this attack, an owner embeds two different watermarks into the same or different host images and uses the singular vectors as the side information or secret keys. In the extracting phase, the malicious actor can extract a fake watermark for each watermarked image by using

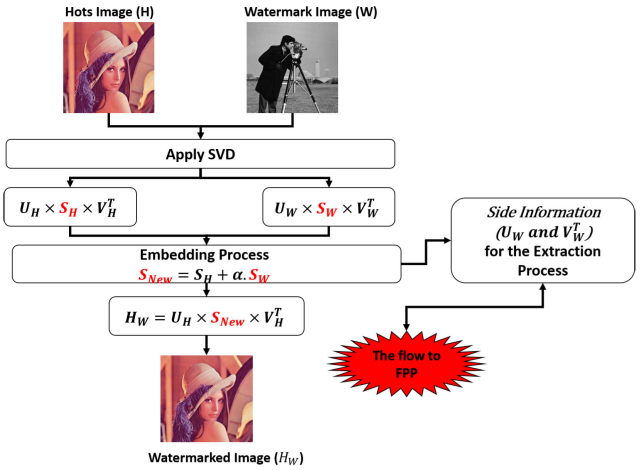

FIGURE 8. The SVMW method of embedding algorithm.

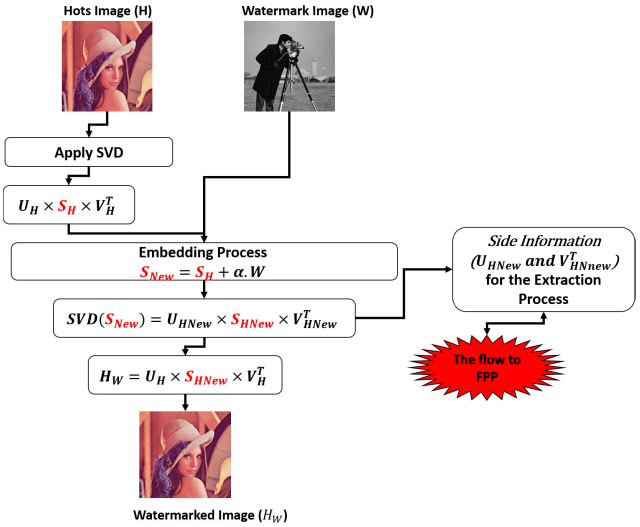

FIGURE 9. The DW type of embedding algorithm.

different singular vectors. Figure 10 depicts this type of attack.

We assume that the two host images are the same ($H_1 = H_2$) while the watermark images differ ($W_1 \neq W_2$). The first watermark W_1 is embedded into the first host image H_1 while the second watermark W_2 is embedded into the second host image H_2. This can be performed using one of the SVMW or DW embedding methods. Both watermarked images H_{W_1} and H_{W_2} have side information that are generated during the embedding process.

During the watermark extraction phase, FFP occurs when the owner can extract the watermark from the watermarked image using different side information. In this case, the second watermark, $W^2_{Extracted}$ can be extracted from the first watermarked image, H_{W_1} using the side information (U_2 and V_2) of the second watermarked image H_{W_2}. At the same time, the first watermark, $W^1_{Extracted}$ can be extracted from the second watermarked image, H_{W_2} using the side information (U_1 and V_1) of the first watermarked image H_{W_1}. Thus, an owner can claim ownership of the image and has strong evidence for doing so. Due to these ambiguity cases, SVD-based image watermarking schemes cannot be used in actual applications that deal with ownership or copyright disputes.

- **Embedding Fake Watermarks**
  In this attack, the owner embeds watermark information W_1 into the host image H, creating the watermarked image H_{W_1}. The side information of the watermark (U_{W_1} and V_{W_1}) will be used in the extraction process. Then, the legitimate owner can distribute the watermarked image H_{W_1} and use the side information as evidence to claim ownership of the image. An adversary can embed fake watermark W_2 into the watermarked image H_{W_1} and also claim ownership of the image. An adversary keeps the side information U_2 and V_2 to use in the extracting phase. Figure 11 illustrates this type of attack.
  At the extraction stage, the adversary can easily prove ownership of the watermarked image by successfully extracting the fake watermark information with high accuracy. Both the real owner and the opponent have strong evidence of claiming ownership of image H. Using this type of attack, many adversaries can effectively embed their watermarks in the same image and demand the actual owner of the image.
- **Extracting Watermarks from Other Images**
  This type of attack extracts the watermark from an arbitrary image that does not contain a watermark. The owner embeds the watermark W into the host image H using the SVD technique, the singular information (U and V) of the watermark are used in the side information during the extraction process. Figure 12 depicts this type of attack. In the extraction process, an owner can use the side information of W to extract the watermark from an arbitrary image that contains another watermark, or even one that does not contain a watermark. An owner can extract the right watermark with a high NC value and claim ownership of the image.

To overcome FPP and other security issues, several solutions have been proposed such as the use of hashing [149], encryption [150], digital signature [144], PCs embedding [123] and singular vector embedding [24].

In the hashing methodology [149], the side information, U_W, and V_W are hashed using a one-way hash function and stored during the embedding process. During extraction, side information used for extraction is hashed and compared against the stored hash values. If they match, the side information is successfully authenticated, and the extraction process can proceed. Otherwise, extraction is aborted.

The use of encryption involves encrypting the watermark prior to the embedding process [150]. During extraction, successful decryption must be performed in order to recover the original watermark. Otherwise, an invalid, arbitrary image will be produced. Schemes that rely on digital signatures to

FIGURE 10. Diagram for attack one (extraction of fake watermarks).

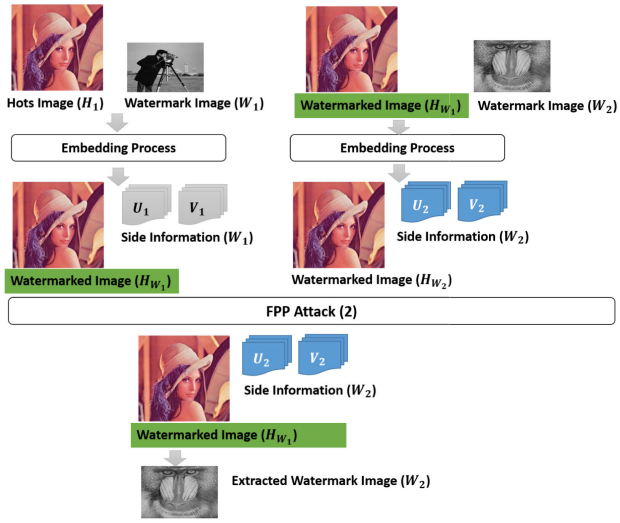

FIGURE 11. Diagram for attack two (embedding fake watermarks).

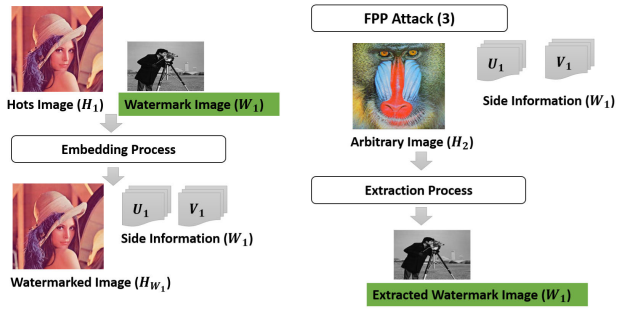

FIGURE 12. Diagram for attack three (extracting watermarks from other images).

prevent FPP [144] still embed watermark information into S_H. In addition, the digital signature of the side information is also embedded into the host image. During extraction, the digital signature can be used to authenticate the extracted watermark.

All of these methods have demonstrated a good trade-off between robustness and imperceptibility. However, these methods still rely on using side information as the extraction key, and may still be susceptible to different variants of FPP. Also, the side information is not sensitive to small changes, which leads to an easy estimation of the watermark. Furthermore, additional authentication processes required during the extraction process incurs computational overhead.

Due to the drawbacks of the aforementioned schemes, new schemes that explicitly address the FPP have been proposed. One of these methods embeds the principal component (PC) instead of the singular matrix, S_W or the watermark itself [123]. PC includes both U and S matrices, whereas the remaining matrix, V is used as the extraction key. The principal component of the watermark, PC_W is generated using SVD and embedded into S_H of the host image. Without V_H, an adversary cannot extract the embedded watermark, thus circumventing FPP. However, this method is vulnerable to geometrical and non-geometrical attacks because U_W holds the structure of the image and has a high sensitivity to small change. Another approach to overcome FPP embeds U_W instead of S_W [24]. The side information, V_W and S_W are used as extraction keys. This method achieves high imperceptibility but is still not robust against different well-known attacks.

Najafi and Loukhaoukha proposed a novel method to solve FPP [151]. They used sharp frequency localized contourlet transform (SFLCT) on the host image and watermark image. SFLCT produces two matrices (approximation sub-band A and details matrix D). The approximation sub-bands of the watermark image A_w is embedded into the approximation sub-bands of the host image A as $A^W = A + \alpha_A A_W$, where α_a denotes the scale factor. At the same time, SVD is applied to two detail matrices D and D_W. The singular values of the watermark, S_W are embedded into the host image as $S^W{}_D = S_D + \alpha_D S_W$. Two watermark matrices are embedded into the host image simultaneously. The watermark can be the same size as the host image. Thus, the FPP is resolved. The proposed method use A, $S^W{}_D$, U_w, V_w as the key for extraction. Consequently, the attacks whereby fake watermarks can be extracted or embedded can be prevented. However, it relies on a large key and SFLCT suffers from high computational complexity.

VII. STATE-OF-THE-ART OF HYBRID SVD-BASED IMAGE WATERMARKING SCHEMES

In the current state-of-the-art, various frequency transforms have been used with SVD to develop new image watermarking schemes. To organize this section, the section is divided into sub-sections according to frequency domains used in the proposed schemes.

A. SVD-ONLY IMAGE WATERMARKING SCHEMES

Aslantas proposed an optimal SVD image watermarking scheme [45] where the DE optimization algorithm is used to generate MSF values to achieve a good balance between robustness and imperceptibility. SVD is first applied to the host image, then watermark information is used to change

the singular values of the host image. The modified singular values are further decomposed by SVD. Then, the resulting singular values are used in the extraction process. Optimal MSF is selected automatically based on PSNR and NC values. The proposed scheme achieves a balance of imperceptibility, robustness and capacity. However, this method still suffers from FPP.

Golea *et al.* [44] proposed an SVD watermarking scheme for color RGB host image and the watermark is color RGB image. The color channels of the host image and watermark image are divided into a set of blocks and SVD is applied to each block of the host image. Embedding is performed by modifying the middle value of the singular values in each host image block based on the pixel values of each watermark image block. The proposed scheme offered good results in terms of imperceptibility, capacity, and robustness against various attacks. However, its easy to extract a embedded watermark and the scheme suffers from FPP.

Lai proposed a robust image watermarking scheme based on SVD and the Tiny-GA algorithm [134]. SVD is used to decompose the host image and the watermark is directly embedded into the singular values of the host image. The scaling factor is selected automatically using Tiny-GA. Results show that the proposed scheme is high imperceptibility, robustness and capacity. However, the FPP security requirements are not taken into account. Jia introduced another color image watermarking scheme based on SVD and secret keys [121]. The RGB watermark image is converted into a binary sequence based on Arnold transformation and secret key. This leads to improved security and robustness. On the other hand, the RGB host image is divided into non-overlapping blocks and each block is decomposed by SVD. The left singular vector U is selected for embedding purposes. The binary series is used to modify the relationship between the second and third values of U matrix. This scheme has high imperceptibility and robustness against different attacks and is circumvents FPP. However, the capacity is low and no analysis is performed to ensure maximal security.

Chung *et al.* [152] introduced two important observations for SVD-based watermarking schemes in order to strengthen imperceptibility and capacity, while altering the U and V^T vectors of the SVD to embed a watermark image. First, for the left singular vector U, altering values of the column vector results in lower distortion as compared to altering values of the row vector. This is because altering column values leads to a small change throughout the matrix as compared to altering the row that focuses on a small localised area of the matrix. For the right singular vector V^T, it is the inverse whereby altering the row values of V^T results in less distortion than altering column values. In the proposed scheme, the authors proposed to modify the column values of U and row values of V^T at the same time. Results indicate that this scheme increased robustness and invisibility.

Fan proposed another SVD scheme without frequency transforms to avoid FPP [130]. SVD is applied to the host image, then vectors U and V are used in the embedding process. The first columns of U and V are changed using watermark information with based on threshold values. FPP is avoided but the robustness and imperceptibility results were not improved as compared to existing work.

B. DWT + SVD-BASED IMAGE WATERMARKING SCHEMES

In [124], a hybrid image watermarking scheme based on DWT and SVD has been proposed. 2-levels DWT is applied to the host image followed by SVD on all sub-bands. The watermark is transformed using 1-level DWT followed by SVD on each sub-band. Then, the principal components are calculated for each sub-band in the watermark. Finally, the principal components of each sub-band are embedded into the singular values S of each sub-band in the transformed host image. DE is used to obtain optimal MSF to achieve imperceptibility and robustness. FPP is avoided as the principal components are used instead of singular values.

Wang and Chen proposed a DWT-SVD image watermarking scheme based on visual cryptography and K-means clustering to protect ownership rights [46]. The host image features are extracted and DWT-SVD is used. These features are classified into two clusters using K-means. The master share is created based on two clusters and used to construct ownership shares. Using (2,2) virtual cryptography and the secret image, create ownership final version. The proposed scheme has low PSNR values which implies a low imperceptibility and high NC values indicating its robustness against attacks.

Li *et al.* [120] proposed a robust DWT-SVD image watermarking scheme to increase imperceptibility and capacity. The human visual model is used to calculate the scale factor. The host image is decomposed by DWT, and SVD is applied to all sub-bands. Singular values of the watermark are embedded into the singular values of the host image's sub-band coefficients. Apart from improved imperceptibility and robustness, the capacity is high because four sub-bands are used in the embedding process. However, this scheme suffers from FPP and has low security against several common attacks.

Dharwadkar *et al.* [43] introduced a non-blind color image watermarking scheme. RGB, DWT and SVD are used in the watermarking scheme. The RGB host image is first decomposed into three channels. Because the blue channel is more robust, it is chosen to apply DWT transform. Finally, the watermark is directly embedded in singular values of the four DWT sub-band coefficients after applying SVD. Its embedding capacity is high because it uses 4 sub-bands, and it is also robust against various attacks. However, the scheme suffers from FPP. Mishra *et al.* proposed another watermarking image by DWT and SVD transformations [26]. DWT is applied three times and SVD is used to decompose the LL_3 matrix. This approach uses the firefly method to generate multiple scaling factors to reach a balance between imperceptibility and robustness.

A new robust image watermarking scheme has been proposed for electrocardiogram (ECG) signals, specifically for

cloud environment [30]. The proposed scheme uses both DWT and SVD on the host image. Watermark information is used to modified the singular values of the DWT coefficients. Results showed that the proposed scheme has excellent PSNR and NC values, implying that the scheme has good security and capacity properties.

Niu *et al.* proposed a color image watermarking scheme based on DWT and SVD [153]. The blue channel is decomposed into seven sub-bands then LL_2 is selected to perform SVD. The watermark is scrambled by Arnold transform and then decomposed by SVD. The singular values S_W are added to the singular values S_H to obtained a new watermarked image. The scheme suffers from FPP. Ojha *et al.* proposed a simple image watermarking scheme based on DWT and SVD [154]. The color host image is transformed to CrCbY color image and region of interest (ROI) is extracted. Both ROI and watermark image are decomposed by DWT, and SVD is applied to get the singular value matrices. The embedding process is performed using SSF and achieves good results. However, the scheme also suffers from FPP.

As human eyes are less sensitive to noise in textured areas, a high-resolution band and image regions with high or low background brightness can be considered when embedding watermarks. Based on these observations, a hybrid image watermarking scheme is proposed [155]. DWT is applied to the host image, LH and HL sub-bands are selected to apply SVD. HVS and logistic map are used to select the optimal locations for embedding. Watermark information is then used to modify the singular values of the optimal area. The proposed scheme achieves high imperceptibility as it leverages upon HVS characteristics. The logistic map is used to encrypt watermark images to improve security and robustness. The embedding process involves two sub-bands, thus increasing the embedding capacity.

Araghi *et al.* [122] proposed a watermarking image scheme based on DWT and 2-levels SVD. The proposed scheme applies DWT on the host image, and the sub-band *HH* is divided into 8×8 non-overlapping blocks. SVD is applied to each block and S_1 of each block is selected to construct a new matrix A. The generated matrix A is also decomposed by SVD. A hash value of the watermark image is calculated using the SVD and DWT to generate a digital signature. Also, S_W of the watermark is used to modify S_1. A digital signature of watermark image that generated by hash value and B test is embedded into the watermarked image. This is performed by first applying DWT then dividing LL into 4×4 non-overlapping blocks. SVD is then applied to 8 randomly selected blocks. Binary values of the digital signature are then embedded into the $V(2, 1)$ matrix. In the extraction process, the user cannot extract the embedded watermark until it passes the two tests (B test and digital signature). The FPP is solved using this 2-levels authentication system. However, as many keys are used in the extraction process, the proposed scheme has high computational overhead.

An image watermarking scheme based on DWT and SVD has been proposed to achieve tamper localization and self-recovery [156]. 1-level DWT is applied to the watermark image and SVD is used on all sub-bands. The principal component $U \times S$ is selected to be embedded into the host image. 3-levels DWT is applied to the host image, and then SVD applied to all sub-bands. The singular values S is modified by the principal component of the watermark image. Scaling factors are obtained using the ABC optimization algorithm to enhance robustness. The LSB of the host image is modified based on tamper localization information to provide self-recovery. This approach solves FPP at the expense of reduced capacity.

Santhi and Thangavelu introduced a new robust DWT-SVD color image watermarking scheme based on the YUV domain [157]. Firstly, the host color image is converted to YUV color space and DWT-SVD are implemented respectively. The watermark image is decomposed by SVD and its singular values are changed to the singular values of the host image. The proposed scheme has good NC values and low PNSR values indicating the watermark can be easily extracted from the watermarked image. However, the scheme has two issues: FPP remains unresolved and it suffers from additional computational overhead.

Dili and Mwangi [158] presented a non-blind DWT-SVD image watermarking scheme. The host image is decomposed by 1-level DWT, the HL and LH sub-bands are selected for the embedding process. The two sub-bands are divided into non-overlapping blocks. Moreover, using a pseudorandom number sequence, two blocks from HL and LH are selected. SVD is applied to these selected blocks and the watermark is embedded into the singular values of the selected blocks. The use of a secret key prevents unauthorised extraction of the embedded watermark. The capacity of the proposed scheme is improved due to the use of two sub-bands. In addition, the proposed scheme has good imperceptibility but is susceptible to many well-known attacks.

Guo *et al.* proposed a watermarking scheme based on DWT and SVD to solve FPP by leveraging upon the principal component of watermark images [159]. The proposed scheme overcomes FPP and the watermark can be easily extracted using side information. However, the scheme has poor capacity, imperceptibility and robustness against well-known attacks. Moeinaddini and Fatemeh proposed an optimized hybrid watermarking scheme based on DWT and SVD [98]. Segmentation and selection of suitable blocks are applied to the host image. DWT and SVD are then used for each block. Opposition and dimension modified firefly algorithm (ODFA) is used to obtain good balance between imperceptibility and robustness. MD5 and AES-192 are used to increase the security of the proposed scheme.

C. DCT + SVD-BASED IMAGE WATERMARKING SCHEMES

Roy and Pal proposed a robust hybrid image watermarking scheme based on DCT and SVD as well as Arnold scrambling [160]. In the proposed scheme, the watermark is scrambled to increase security, and then, the host image and scrambled watermark are divided into a set of non-overlapping blocks.

Every four blocks, the first block is selected for the watermark embedding process. All selected blocks transferred into DCT domain and SVD is applied to these coefficients of the host image and watermark image. The singular values are exchanged after multiplying by a scaling factor. The proposed scheme offered good imperceptibility and robustness results, as well as the scheme is secure because the watermark image is scrambled before the embedding process.

A new hybrid watermarking scheme based on SVD, DCT, and HVS has been proposed [129]. The host image is divided into 8×8 blocks and calculated HVS entropy and edge entropy values and ordered in ascending order. DCT is applied and the coefficients are used in SVD. SVD is applied to each block and the $U(3, 1)$ and $U(4, 1)$ are changed based on the series of watermark bits and threshold value through an examination of these values. The FPP is solved as the proposed scheme did not use S value. However, small size of the watermark, which is embedded using U is more sensitive to change and weak under different attacks.

A new hybrid scheme based on DWT, SVD, and Human visual system (HSV) has been proposed [161]. The watermark image is binarized with size 32×32 bits and the host image is divided into 8×8 blocks with different coordinates (x, y). The coordinates are encrypted using the AES. Each block calculates the entropy and edge entropy values and it is sorted in ascending order. 1024 blocks are selected that have the lowest values in the embedding process. DWT is applied to each of the selected blocks and LL is selected to apply SVD. $U(2, 1)$ and $U(3, 1)$ are selected and examined to embed the watermark based on the threshold value. The FPP is solved by using U during the embedding process. However, the watermark has limited size and changes based on U values only.

Balasamy and Suganyadevi [162] presented a new medical image watermarking scheme based on DWT and SVD. The ROI was selected based on the fuzzification method. A watermark is converted to frequency coefficients and the sub-band is encrypted using the logistic map. The key component is calculated to avoid FPP attacks. The singular values of both images are modified based on the key. Results indicate the proposed scheme has excellent results in terms of robustness and imperceptibility.

A new hybrid scheme based on DWT and SVD has been proposed in [163]. The watermark image is decomposed using SVD, and the host image is transformed for 4-level DWT. SVD is then applied to LL_4. The singular values are embedded into the singular values of the host image under the optimum MSF parameters generated by a PSO algorithm. However, the proposed scheme suffers from FPP, and is susceptible to well-known attacks.

D. DWT + DCT + SVD-BASED IMAGE WATERMARKING SCHEMES

Singh *et al.* [164] proposed a robust image watermarking scheme that embeds a watermark image and a watermark text into a medical host image. Firstly, the host image undergoes a 2-levels DWT. The watermark text is encrypted by ASCII representation and embedded into HH. The rest of the sub-bands are decomposed by DCT and SVD respectively, and the watermark medical image is also decomposed by DCT and SVD in the same order. Singular values of the watermark are used to modify the singular values of the host image. The scheme has low imperceptibility but NC values under different attacks show high robustness. The proposed scheme has higher capacity as it can embed two watermarks. The proposed scheme provides excellent robustness, and the scrambled watermark image provides high security. Moreover, based on the size of the watermark image, the capacity can be varied.

A hybrid watermarking scheme is proposed in [28] for medical images. Both the host image and watermark are transformed by a 3-levels DWT followed by DCT and SVD. The watermark's singular values are inserted into the host image's singular values in the high frequency sub-band. This proposed scheme offers a good trade-off between imperceptibility and robustness. However, it suffers from FPP because only the singular values are used. The capacity of the scheme is not introduced nor analyzed. Fazli and Moeini proposed another watermarking scheme based on DCT, DWT, and SVD [140] in which the host is divided into four parts equality. DWT and DCT are applied to each part, and a new matrix is generated by collecting the first two alternating current (AC) coefficients. The watermark is scrambled by Arnold transform and embedded directly into the singular values of all four parts. This scheme is robust against watermark attacks, and its capacity is improved as it embeds a watermark into four parts of the host image. However, the proposed scheme suffers from FPP.

The image watermarking scheme proposed in [19] has three embedded watermarks, one being an image (logo) while the other two are textual patient information. DWT is applied to the host image, LH_1 is selected, then DCT is applied. SVD is then applied to the DCT coefficients. The singular values of LH_1 are changed using singular values of the medical image. The medical image is scrambled using the Arnold transform for improved security. Also, patient information is transformed into binary data and compressed. Back propagation neural network (BPNN) is used during the extraction of the watermark image to withstand various attacks. Their scheme does not address FPP and requires multiple keys for the extraction process.

Kang *et al.* [84] also proposed a hybrid watermarking scheme based on DWT, DCT, and SVD. DWT is applied to a host image and then the transformed image is divided into 8×8 non-overlapping blocks. DCT is applied to each block, and the middle frequency is extracted to form a 2×4 matrix. The matrix is further divided into 2×2 sub-matrices, to which SVD is applied. The largest singular values of the two matrices is modified using bits from the watermark image. The watermark image is encrypted using a logistic map prior to the embedding process. The scheme achieves a good trade-off

between imperceptibility and robustness. However, the FPP still persists.

The image watermarking scheme based on SVD, DCT, and DWT proposed by [13] first converts a host image using a 2-levels DWT. DCT and SVD are applied to the approximation sub-band of the 1-levels. The watermark image is converted using 1-level DWT, followed by the application of DCT and SVD to the approximation sub-band. The singular values of the watermark image are used to modify the singular values of the host image. Next, a text watermark is transformed into a binary stream and encrypted. Text watermark information is embedded into the diagonal sub-band of the 2-levels of DWT. The extraction process follows the same order albeit with different calculations. However, the proposed scheme does not resolve the FPP.

Zhang *et al.* [139] proposed a hybrid watermarking scheme where the host image is first transformed by a 1-level DWT, then LL is divided into 8×8 blocks. DCT is executed for each block. DCT is applied again on the 4×4 block located in the upper-left coefficients. Blocks in the upper-left side of each coefficient with equivalent size to the watermark is selected. SVD is applied to these blocks and the resulting W values are used to modify S of the host image as $SVD(S + a.W) = U_2 S_2 V_2$. Then, S_2 is used instead of the S_1 in the host image. The watermarked image is encrypted using Arnold transform. One of the advantages of the proposed scheme is that a watermark can be of any size. The FPP is addressed via encryption. However, the proposed scheme requires many additional operations, leading to unnecessary computational overhead.

The watermarking scheme proposed by [119] embeds two different watermarks (image and text) into a host medical image. First, 2-levels DWT is applied to the host image, followed by DCT and SVD. On The watermark image is decomposed by DCT and SVD using the same procedure. The text watermark is encrypted before being embedded into the HH sub-band of the 2-levels of DWT. The singular values of the host image are then exchanged with the singular values of the watermark image. The proposed scheme has low imperceptibility and a high level of robustness under different attacks. Furthermore, the scheme has high capacity as it is capable of embedding two watermarks.

Chaitanya *et al.* [25] proposed a new color image watermarking scheme based on DWT, DCT, and SVD. 2-level DWT transform is applied on the blue color channel of the host image. The median energy of a sub-band is selected and DCT is applied to it for the embedding process. The watermark image and DCT coefficients of the host image are decomposed by SVD and the singular values of the watermark are embedded into the singular values of the host image. However, FPP was not addressed and there is a lack of robustness against other attacks.

E. IWT/LWT + SVD-BASED IMAGE WATERMARKING SCHEMES

In their watermarking scheme, [113] applied IWT to the host image and SVD to all sub-bands. Arnold transform is used to scramble the watermark for increased security. Then, the scrambled watermark is directly embedded into the singular values of the host image. In a separate scheme proposed to address FPP, [112] used IWT and SVD to embed a watermark. A signature is generated from two singular vectors of the embedded image. The signature is verified before the watermark is processed in the extraction phase. Another approach based on IWT which aims to overcome the FPP embeds U_W instead of S_W [24]. The side information, V_W and S_W are used as extraction keys. This method achieves high imperceptibility but is not robust against several well-known attacks.

Arumugham *et al.* [165] proposed a watermarking scheme based on IWT and SVD, where the watermark image is an integration of the ID number and thumb impression of a patient. The watermark image is encrypted based on a digital chaotic map (Lü Attractor and Tent map). Ansari *et al.* proposed new method to solve FPP in SVD-based watermarking scheme [137] where IWT is used to decompose the host image into four sub-bands, and SVD is performed on three sub-bands (LL,HL, and LH). The singular vectors are used to generate the signature values (to address FPP) and ABC algorithm is used to select the optimal scale factor.

F. OTHER TRANSFORMS + SVD-BASED IMAGE WATERMARKING SCHEMES

A new watermarking scheme based on Tucker decomposition and SVD has been proposed by [131]. The color host image is decomposed by a third-order tensor and the first feature image is selected because it is more stable. The first feature image is divided into non-overlapping 3×3 blocks, to which SVD is applied. At the same time, the original color watermark is scrambled using the Arnold map and all the pixel values are transformed into a single scrambled bit sequence. The watermark image bits are embedded by changing U of each block. Two threshold parameters are used for coefficient comparison to extract the watermark image. However, the scheme has low security against geometrical and non geometrical attacks, and can only embed a small watermark.

A new image watermarking scheme based on non-subsampled contourlet transform (NSCT), redundant discrete wavelet transform (RDWT) and SVD is proposed in [133]. The host image is first sampled by a sub-sampling method. The entropy of these samples are computed and NSCT is applied to the sample with maximal entropy. RDWT is applied to the high frequency portion of the HH sub-band of NSCT image, and SVD is applied to the selected sub-bands of RDWT components. Then, S is selected for the

embedding process. Two watermark images (image watermark + electronic patient record (EPR) watermark) are transformed by NSCT and RDWT. Then, SVD is applied to the watermark images to produce S. The watermark images are then encrypted using a 2D logistic map. The proposed scheme can withstand various attacks but the FPP is not resolved. In addition, the encryption process is subpar as it does not fulfill diffusion and confusion properties.

A new image watermarking scheme based on DWT, scale-invariant feature transform (SIFT) and SVD are proposed in [128]. This scheme extracts invariant features by performing the DWT, SVD and SIFT on the host image. In the first phase, 3-levels of DWT is applied to the host image. The LL_3 sub-band is selected for further processing. Using PRNG, $N \times N$ pixels of LL_3 are selected. Then, SVD is performed on windows of 7×7 pixels. The maximum S values are then collected to create a new matrix, A. In the second phase, SIFT is applied to LL_3 to obtain robust key points. SVD is then applied and the four larger S values are selected to create 2×2 blocks of a new matrix B. In the third phase, blocks of B are replaced with blocks of matrix A in a uniform manner. In order to support multiple cover images, these phases are repeated to create n feature shares $F1$,$F2, \ldots, F_n$ to construct a new secret share. The XOR bit-wise operation is used between the three components feature shares, key, and watermark. The $(n+2, n+2)$ visual cryptographic shares are used with XOR operation to construct a general secret share. The general share can be registered with a centralised trust authority for further authentication. This type is called zero watermarks with no embedding data. However, the proposed scheme incurs additional computational overhead.

Reference [27] proposed a hybrid robust image watermarking scheme based on redistributed invariant discrete wavelet transform (RIDWT) and SVD transforms, and the ABC optimization algorithm. In this scheme, 1-level of RIDWT is applied to the host image. The LL sub-band is then selected and divided into non-overlapping blocks. To select optimal blocks, HVS is used in the embedding process. Next, SVD is used on the optimal blocks, and the U vector is used in the embedding process. The U elements are modified based on principal component with an optimized scale factor. A compensating method is used on V_T vectors to decrease the visual distortion. The results showed very good robustness and imperceptibility. Security and capacity are improved compared to other schemes.

Reference [166] proposed a scheme that embeds two identical watermark images. DWT and all phase discrete cosine biorthogonal transform (APDCBT) are applied to the host image to generate a new matrix, DC. SVD is then used to complete the embedding process. Ali *et al.* proposed a zero watermarking scheme based on various transformations such as RIDWT and discrete fractional Fourier transform (DFrFT) [127]. After applying these transforms, SVD is applied to random positions of LL, selected using the secret key as seed. The largest singular value of each position is collected and averaged. The average value is used to generate a binary map. Finally, the master share and watermark images are XORed to generate the owner's share. Rawat and Raman proposed a zero watermarking scheme based on visual secret sharing, fractional Fourier transform (FrFT) and SVD [167]. Two image shares are constructed and SVD is used to extract features of the host image.

Reference [168] proposed a new color image watermarking scheme where the color host image is converted to YCBCr form, and the I_y component is selected and scrambled using the Arnold chaotic map. RDWT is applied, followed by SVD on LL_y. The PC of LL_y is computed as $I_{pc} = U_{LL} * S_{LL}$. The color watermark image that has the same size as the host image is scrambled by the Arnold chaotic map, and then converted to YCBCr form. The new converted watermark image, W_y and LL_y of the host image are used to generate a strength scale factor based on the ABC optimization algorithm. The converted watermark with said strength scale factor is embedded into the PC, I_{pc} of LL_y as $I_{pc} = I_{pc} + \alpha \times W_y$. Next, SVD is applied to the new result, I_{pc}, and the obtained singular values S_{LL} is used instead of S_{LL} in LL_y. The proposed scheme is a new embedding scheme with excellent embedding capacity. However, the proposed scheme still suffers from FPP and low robustness against well-known attacks.

Reference [169] proposed a new color image watermarking scheme based on translation invariant wavelet (TIW) and SVD transforms. The color host and watermark images are decomposed by TIW, and the LL sub-bands of the RGB color channels are selected for the embedding process. The MSF parameters are optimized by using the enhanced grey wolf optimizer (E-GWO) algorithm. Embedding capacity is improved and the imperceptibility is high. However, the embedding is conducted using the SVMW method which is susceptible to FPP attacks.

In [12], two robust color image watermarking schemes are introduced based on DWT and SVD transforms. The first scheme is based on a homomorphic transform, DWT and SVD. A 1-level DWT is applied to the host image and the resulting LL sub-bands are extracted to each of the RGB components. A homomorphic transform is applied to the RGB channels. Then, SVD is applied to each of the channels. The watermark image is directly embedded into the singular values. The second scheme is a hybrid technique where 3-levels of DSWT in DCT domain are applied to each component of the host image. Four sub-bands are obtained, each having the same size of the host image. The obtained four sub-bands are the A, H, V, and D matrices. The watermark image is then embedded into the matrix, A. The proposed scheme has high NC values against various attacks. However, it suffers from low PNSR and security because the watermark image is directly embedded.

VIII. COMPARISON AND CRITICAL ANALYSIS

Many of SVD-based watermarking schemes have been proposed based on different frequency transformations. Initially, we provide some general observations with regards to SVD-based schemes. First, frequency transform is the major

component used before SVD is applied to reduce distortions. Most existing schemes utilize DWT or DCT before applying SVD, to improve imperceptibility and robustness. Some frequency transforms are also used in some of the schemes that have some required characteristics.

The second observation that we have made is that the *LL* sub-band is most commonly used sub-band for embedding as it will an approximation of the original image. Thus, the embedding process will have a minimal effect on the original image but the its embedding capacity is restricted to less than a quarter of the host image size. On the other hand, other sub-bands have been used in other schemes to maximize embedding capacity. However, the embedded watermark will be susceptible to a number of attacks. High-resolution sub-bands have also been used for embedding purposes. They have been used to embed text watermarks or digital signatures for authentication purposes. Overall, *LL* is shown to be the most robust to attacks and results in smaller distortions.

In order to increase the security of watermarks, the encryption of watermark data prior to embedding has been applied in several schemes. The Arnold and Logistic maps are commonly used to scramble image pixels. In addition, the ASCII code is used to encrypt the watermark text [170]. PRNGs are used in several schemes for encryption or to select blocks for embedding purposes. However, the use of scrambling algorithms for encryption does not provide adequate security.

Watermarks can be of various types such as images or text. Watermark images themselves can be of various types such as binary, gray scale, RGB color image, X-ray image, logo image, and others. Some schemes switch between color schemes (RGB to YUV) to improve imperceptibility. Image sizes affects the embedding capacity of a watermarking scheme. For example, binary or logo images have smaller sizes as compared to a grayscale or a color image. Some schemes embed two watermark images in different sub-bands, while others embed a combination of images and text such as in medical watermarking schemes. High capacity is required to ensure that the rightful owner is protected, while low capacity implies that a watermark is easily destroyed.

There are various approaches for embedding watermark information in the three SVD coefficients. Most schemes are based on the SVMW and DW methods because the singular values are more stable as compared to singular vectors. Nevertheless, the SVMW and DW methods suffer from FPP, which make it easy to extract a fake watermark from the watermarked image. The CT method is robust against well-known attacks and has elevated imperceptibility because it produces slight alterations in the left singular vectors. However, it has a limited capacity due to a change to one or two U values. The PC method has a large capacity and is effective against FPP attacks. However, under different attacks, it is weak and needs a larger keyspace to be secure.

The SVC method used singular values with other conditions to embed watermark information. However, these schemes still suffer from FPP. Zero watermarking strategies make it easier to overcome FPP because no embedding is done in the host image. In this case, the owner can protect original content of the host image from any alteration. However, attackers may demand to have their watermarks extracted using this method and claim ownership as there is no embedding is performed in the host image itself. In other methods, U, V or both are used for embedding purposes.

Scale factors play a role in managing robustness and imperceptibility. SSF and MSF are widely used in various schemes. However based on our findings, SSF cannot achieve a desirable trade-off between robustness and imperceptibility. On the other hand, MSF has a can lead to good trade-offs between various watermarking requirements. Intelligent optimization algorithms are used to achieve optimal MSF values by using PSNR and NC to determine fitness. Different optimization algorithms are used in the watermarking schemes such as ABC, PSO, DE, GA, K-means Algorithm and Firefly Algorithm. Nonetheless, every watermark has its own optimal MSF value which needs to be maintained as the key for extraction purposes.

Lastly, blocking strategies are commonly used in SVD-based watermarking schemes for improved security. A non-overlapping blocking strategy is applied to the host image or the watermark image in the spatial or frequency domain. A block has various sizes, but most schemes rely on 8×8 blocks. A blocking strategy plays an important role in improving flexibility in terms of the embedding process. Tables 9, 10 and 11 provide a list of 72 SVD-based watermarking schemes that have been proposed in the last two decades. The eight previously mentioned criteria are used in the table to differentiate between these schemes. In order to visualize a professional comparison, Figure 13 displays the percentage between these criteria to help us recognize obstacles and weaknesses.

According to existing literature, hybrid SVD-based image watermarking schemes are effective when used with other frequency transforms, particularly DWT and DCT. In other words, the hybrid SVD and other transforms have proven superior to SVD-based spatial watermarking schemes in terms of imperceptibility, robustness, security, and capacity. Security in hybrid SVD-based watermarking schemes is an essential requirement. Consequently, various SVD embedding strategies are used to avoid FPP and resist numerous geometric and non-geometric attacks. Furthermore, optimization algorithms are commonly used to generate optimum MSF for good trade-offs between imperceptibility and robustness. It automates the search for optimal MSF values and compensation thresholds after the execution of different attack tests.

Next, we will highlight how well existing schemes fulfill the four watermarking requirements (security, robustness, imperceptibility, capacity). Firstly, preventing FPP is vital to ensure that a watermarking scheme is secure. Unfortunately, many proposed schemes did not discuss or address the issue. Some of the prevention or avoidance strategies which can produce better results can be categorized into three classes as shown in Figure 14 and detailed below:

TABLE 9. Comparison of existing SVD-based watermarking schemes.

No.	Scheme	Type of transforms	Embedding Sub-bands	Watermark Encryption	Watermark type and size	Embedding Method	Exist FPP	Optimization algorithm	Blocking
1	[120]	DWT,SVD, and HVM	All	No	Gray image with size 256×256	SVMW	Yes	No	No
2	[46]	DWT, SVD, K-means and VC	LL	No	Binary image with size 64×64	Zero	No	No	No
3	[45]	SVD	-	No	Gray image of size 32×32	DW	Yes	Yes(DE)	No
4	[44]	SVD	-	No	RGB color image of size 32×32	SVC	Yes	No	Yes
5	[43]	DWT and SVD	All	No	Monochrome image of size 200×150	SVMW	Yes	No	No
6	[134]	SVD	-	No	Gray image of size 64×64	DW	Yes	Yes(Tiny-GA)	No
7	[121]	SVD	-	Yes (Arnold Scrambling)	RGB color image of size 32×32	CT	No	No	Yes
8	[159]	DWT,SVD and SSVD	LL	No	Gray image of size 64×64	PC	Yes	No	Yes
9	[51]	DCT and SVD	DC coefficients	Yes(Arnold Scrambling)	Gray image of size 64×64	DW	No	Yes(DE)	Yes
10	[26]	DWT and SVD	LL	No	Binary image with size 32×32	SVMW	Yes	Yes(Firefly)	No
11	[27]	RIDWT, HVS and SVD	LL	No	Binary image with size 32×32	CT	No	Yes (ABC)	Yes
12	[30]	DWT and SVD	All	NO	Logi image with size 77×77	SVMW	Yes	No	No
13	[164]	DWT, DCT and SVD	HH and LL	Yes(ASCII)	Gray image with size 256×256	DW	No	No	No
14	[160]	DCT and SVD	-	Yes(Arnold Scrambling)	Binary image with size 128×128	SVMW	Yes	No	Yes
15	[12]	DWT, SVD and Homo-morphic transform	LL	No	RGB color image of size 512×512	SVMW with adding S of host image	Yes	No	No
16	[28]	DWT, DCT and SVD	HH	NO	Binary image with size 512×512	SVMW	Yes	No	No
17	[19]	DWT, DCT and SVD	LH1,LH2 and LL3	Yes (Arnold Scrambling) and Hamming error correction code	Lump image 256 × 256 text watermark 190 characters	SVMW	Yes	Yes (BPNN)	No
18	[146]	DWT and SVD	All	No	Gray image with size 256×256	SVMW	Yes	No	No
19	[29]	DWT and SVD	LH and HL	No	Gray image with size 128×128	DW	Yes	No	No
20	[95]	FRRT, DWT, and SVD	All	No	Binary image with size 33×33	SVMW	Yes	No	No
21	[171]	RDWT and SVD	All	No	Gray image with size 512×512	SVMW	Yes	No	No
22	[65]	RDWT and SVD	All	No	Gray image with size 512×512	DW	Yes	No	No
23	[113]	IWT and SVD	All	Yes (Arnold Scrambling)	Gray image with size 256×256	DW	No	No	No
24	[172]	LWT and SVD	LH3	No	Binary image with size 32×32	SVMW (Hash U and V)	No	Yes (MOGAO)	No
25	[150]	LWT and SVD	HH, LH, HL	Encrypt	Binary image with size 32×32	SVMW (Hash U and V)	No	Yes (ACO)	No

TABLE 10. Comparison of existing SVD-based watermarking schemes (continued).

No.	Scheme	Type of transforms	Embedding Sub-bands	Watermark Encryption	Watermark type and size	Embedding Method	Exist FPP	Optimization algorithm	Blocking
26	[135]	DWT, DCT, and SVD	All	No	Gray image with size 256×256	PC	No	Yes (PSO)	No
27	[125]	DWT and SVD	LH3	Encrypt	Binary image with size 32×32	SVMW (Hash U and V)	No	Yes (MOGAO)	No
28	[112]	IWT and SVD	All	No	Gray image with size 256×256	DW (Signature embedding)	No	No	No
29	[161]	DWT, SVD and HSV	LL	No	Binary image with size 32×32	CT	No	No	Yes
30	[126]	DWT, SVD and HVS	LL3 and HH3	Yes (Arnold Scrambling) and Otsu's method	Binary image with size 64×64	DW and Zero embedding	No	Yes (DE)	No
31	[124]	DWT and SVD	All	No	Gray image with size 256×256	PC	No	Yes (SDE)	No
32	[147]	DWT and SVD	LH3	No	Binary image with size 32×32	PC	No	Yes (PSO)	No
32	[148]	RDWT and SVD	LL	No	Gray image with size 512×512	PC and SVMW	No	No	
34	[152]	SVD	-	No	Binary image with size 32×32	CT	No	No	Yes
35	[130]	SVD	-	No	Binary image with size 32×32	CT	No	No	Yes
36	[129]	DCT and SVD	-	No	Binary image with size 32×32	CT	No	No	Yes
37	[144]	DWT and SVD	HH	No	Gray image with size 256×256	SVMW (Signature) and replace the singular values based on blocks	No	No	Yes
38	[123]	SVD	-	No	Gray image with size 256×256	PC	No	No	No
39	[145]	SVD	-	No	Gray image with size 200×200	DW	Yes	No	No
40	[24]	IWT and SVD	LL	No	Gray image with size 256×256	U embedding	No	Yes (MOGAO)	No
41	[151]	SFLCT and SVD	All sub-bands	No	Gray image with size 512×512	SVMW + DW	No	No	No
42	[131]	Tucker and SVD	-	Yes (Arnold Scrambling)	RGB color image of size 32×32	U embedding	No	No	yes
43	[84]	DWT, DCT and SVD	LL	Yes (Logistic map)	Gray image with size 32×32	SVMW +CT	No	Yes (LSCF)	yes
44	[122]	DWT and SVD	HH + LL	No	Gray image with size 64×64	SVMW + V embedding	No (Hash and signature)	No	yes
45	[133]	NSCT, RDWT and SVD	HH	Yes (Logistic map)	Thorax image with size 256×256 and EPR image with size 128×128	SVMW	Yes	No	No
46	[156]	DWT and SVD	all sub-bands	No	X-ray with size 128×128	PC	No	Yes (ABC)	No
47	[13]	DWT, DCT and SVD	LL	yes	Gray image with size 512×512 and 128 characters	SVMW	Yes	No	No
48	[128]	DWT, SIFT and SVD	LL	No	Binary image with size 64×64	Zero and SVMW	No	No	Yes
49	[139]	DWT, DCT and SVD	LL	Yes (Arnold Scrambling)	Gray image with size 128×128	DW	No	No	Yes

TABLE 11. Comparison of existing SVD-based watermarking schemes (continued).

No.	Scheme	Type of transforms	Embedding Sub-bands	Watermark Encryption	Watermark type and size	Embedding Method	Exist FPP	Optimization algorithm	Blocking
50	[165]	LWT and SVD	LL	No	Binary image with size 256×256	DW	Yes	No	No
51	[140]	DWT, DCT and SVD	All sub-bands	Yes (Arnold Scrambling)	Four Binary image with size 32×32	DW	No	No	Yes
52	[98]	DWT, HVS and SVD	LL	Yes (MD5 hash+ PRNG)	Binary image with size 32×3	CT	No	Yes (ODFA)	Yes
53	[166]	DWT, APDCBT and SVD	LH and HL	No	Two binary images with size 32×3	DW	Yes	No	Yes
54	[127]	RIDWT, DFrFT, VSS and SVD	LL	No	Two binary images with size 64×64	Zero	No	No	Yes
55	[167]	FrFT, VSS and SVD	-	Yes (PRNG)	Two binary images with size 64×64	Zero	No	No	Yes
56	[153]	DWT and SVD	LL	Yes (Arnold Scrambling)	Gray image 256×256	SVMW	Yes	No	No
57	[137]	IWT and SVD	All sub-bands	No	Gray image 256×256	SVMW+DW	Yes (Signature)	Yes (ABC)	No
58	[154]	DWT and SVD	All sub-bands	No	Gray image 256×256	SVMW	Yes	No	No
59	[157]	DWT and SVD	All sub-bands	YUV color Space	Gray image 256×256	SVMW	Yes	No	No
60	[119]	DWT, DCT and SVD	All sub-bands	Yes(ASCII)	-	SVMW + HH embedding	Yes (image)	No	No
61	[155]	DWT, HSV and SVD	LH and HL	Yes (Logistic map)	Binary image with size 128×128	DW	No	No	No
62	[158]	DWT and SVD	LH and HL	No	Binary image with size 16×16	SVMW	Yes	No	Yes
63	[25]	DWT, DCT and SVD	LH, HL and HH	No	Gray image with size 64×64	SVMW	Yes	No	No
64	[89]	DCT and SVD	DC coefficients	No	Binary image with size 64×64	Zero	No	No	Yes
65	[90]	DCT and SVD	DC coefficients	No	Binary image with size 32×32	SVMW	Yes	No	Yes
66	[22]	QHT and Schur (Enhanced SVD)	Unitary matrix	No	Binary image with size 64×64	CT	No	No	Yes
67	[108]	DWT and SVD	All	No	Binary image with size 64×64	DW	Yes	No	Yes
68	[109]	RDWT and SVD	All	Yes	Binary image with size 256×256	DW	Yes	No	Yes
69	[162]	DWT and SVD	All	Yes (logistic map)	gray image with size 256×256	SVMW + PC	No	No	No
70	[163]	DWT and SVD	LL4	No	medical image with size 32×32	SVMW	Yes	Yes (PSO)	No
71	[168]	RDWT and SVD	LL	Yes (Arnold Scrambling)	color image with size 512×512	SVMW	Yes	Yes (ABC)	No
72	[169]	TTW and SVD	LL	No	Color image with size 256×256	SVMW	Yes	Yes (EGWO)	No

1) **Embedding Methods**
A watermark image is decomposed using SVD, and the singular vectors U and V are embedded in the host image. One of the singular vectors, both singular vectors, or the principal component US can be embedded. The remainder of the SVD components can be used as a key. To use this FPP prevention method, the watermarking schemes need to rely on optimization algorithms to identify optimal MSF parameters. However, modifying a few U or V values based on threshold values and the compensation procedure limits the embedding capacity [24], [98], [122].
2) **Encryption Methods**
A watermark images have been encrypted in one of three ways: the first is via XOR with a key-stream generated from a PRNG, the second is by scrambling image pixels based on chaotic map outputs, and the third is by using conventional encryption algorithms such as AES. Encryption methods need to be further investigated as scrambling and XOR-based encryption may not be sufficient. On the other hand, small distortions will lead to authentication problems if conventional cryptographic algorithms are used [19], [133], [139].
3) **Authentication Methods**
Digital signatures are created from SVD components to be saved as a key or embedded into the host image. In this method, the extraction and verification of the signature is required before the extraction of the watermark algorithm. Although effective, these additional authentication steps incur additional computational overhead. In addition, distortions of the signature can affect the extraction process [98], [122], [137], [164].

In terms of robustness, there are some key points in existing schemes that can be identified. Some of them are highlighted as follows:

- Hybrid transforms with SVD are used to improve robustness to multiple well-known attacks [128], [139].
- After decomposing a watermark using SVD, one of the SVD components is used for embedding purposes which reduces direct distortions to the watermark image [13], [24], [156].
- A blocking strategy is successful in enhancing robustness because it decreases the distortions to the host image as a whole [128], [139], [166].
- Optimization algorithms are used to balance robustness and imperceptibility [84], [98], [156].

The first three points are critical in the design of new watermarking schemes. The use of optimization algorithms leads to reduced efficiency as unique MSF values need to be generated for each watermark.

In terms of imperceptibility, there are some key points that can be highlighted:

- HVS is used in many schemes to select the best regions to minimize visual distortions in watermarked images [98], [120], [126], [161].
- Modifying the singular values of the host image helps to reduce visual distortions [133], [153], [154].
- Modifying $U(1, 2)$ or $U(1, 3)$ with the help of threshold values and compensation can improve imperceptibility [27], [129], [156].
- Optimization algorithms are used to obtain a good trade-off between robustness and imperceptibility [84], [98], [156].
- Using solely SVD can lead to improved imperceptibility [121], [159].
- A blocking strategy is successful in enhancing imperceptibility because it decreases the distortion of the image as a whole [128], [139], [166].

Lastly, capacity plays a role in balancing watermarking requirements in SVD-based watermarking schemes. Large embedding size leads to low imperceptibility and improved robustness. Conversely, a small embedding size leads to high imperceptibility and decreased robustness. To obtain a high capacity while balancing other requirements, various schemes have relied upon blocking strategies [128], modification of singular values [28], embedding multiple watermarks [133], [166], embedding into color images [12], [121], and using several sub-bands for embedding purposes [112], [124].

For performance comparison, existing schemes used geometrical and non-geometrical attacks to evaluate the robustness while NC test and PSNR values were always used to evaluate imperceptibility. In this comparison, we select six common attacks that most schemes use for evaluation. These attacks include JPEG compression, median filtering, salt and paper noise, re-scaling, histogram equalization, Gaussian noise, and cropping. PSNR values are also collected from these existing schemes. Tables 12 and 4 provide a performance comparison for most of the existing schemes included in the critical analysis. Some of these schemes lack results, implying that more study is required for the proposed scheme to verify security or performance claims. Table 12 covers existing schemes that did not employ optimization search algorithms in their designs whereas Table 4 provides a comparison of existing schemes that employ optimization search algorithms in their designs to find suitable scaling factors for achieving a trade-off between robustness and imperceptibility. The results for watermarking schemes that rely on optimization are better than those that do not. Therefore, the design of improved schemes that depend on the embedding methods rather than optimization algorithms to achieve desirable trade-offs between watermarking requirements still remains an open problem.

The visual performance comparison in Figure 15 consists average values of the six attacks according to three strategies, blocking, optimization and encryption, which are commonly used in existing schemes. The average PSNR values for

FIGURE 13. The percentage between the criteria of the comparison of existing SVD-based watermarking schemes.

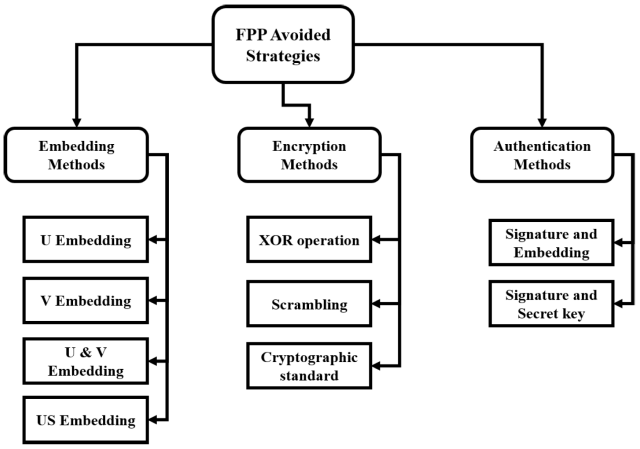

FIGURE 14. Classification of FPP prevention.

existing schemes according to those three techniques is also calculated. Some main points can be summarized as follows:

- Schemes that rely on the blocking technique are less robust against attacks as compared to that schemes that do not. This low robustness can be attributed to the embedding process that involves small non-overlapping blocks that are weak against attacks. In contrast, non-blocking strategies embed data in all frequency coefficients (distributed in all singular values of sub-band coefficients) which leads to improved resistance against attacks.
- Existing schemes that rely on optimization algorithms have better results than existing schemes that do not. Optimization algorithms help identify optimal scaling factors that achieve better trade-offs in watermarking requirements.
- Existing schemes that used encryption methods to protect the watermark image are still susceptible to some of the attacks such as cropping, Gaussian noise, salt and paper noise and JPEG compression because encryption algorithms make significant changes to the watermark image.
- Schemes that rely on all three strategies simultaneously have large PSNR values as compared to other schemes because these strategies play a role in maintaining image quality after the embedding process in hybrid SVD-based image watermarking schemes.

IX. RESEARCH GAP

Several studies addressing the FPP and trade-offs between watermarking requirements in SVD-based image watermarking schemes have been proposed. These studies used different strategies to solve the FPP such as encryption, hashing, signature, embedding singular vectors, and PCs. However, these strategies have drawbacks such as the need for additional authentication operations [112], [122], [144], the lack of security properties (diffusion and confusion in encryption methods) [84], [131], and high sensitivity to small changes to singular vectors [98], [122].

In terms of trade-offs, optimization algorithms are used to achieve the desirable result [84], [98], [156] by identifying optimal MSF parameters. The optimal MSF parameters must be kept as the key for the extraction phase. However, optimal MSF parameters are not flexible to changes in the watermark information. This means that the scheme needs to recalculate new MSF values if there are small changes to the watermark. To provide higher flexibility, new strategies need to be investigated where MSF parameters are not kept as a key [98], [167].

Thus, further research work is still required to design SVD-based watermarking schemes that can overcome FPP without additional authentication operations, improving the security of any underlying encryption operations, as well as achieve good trade-offs without the use of optimization algorithms. As of now, existing schemes have not been able to address these noteworthy issues.

X. DISCUSSIONS AND RECOMMENDATIONS

The trade-off between watermark requirements is the biggest challenge for researchers, whereby a balance needs to be struck between robustness and imperceptibility as well as security and capacity. Here are some recommendations that can be taken into consideration when designing new watermarking schemes:

1) In order to avoid FPP in SVD-based watermarking schemes and improve embedding capacity, watermark information should be encrypted prior to embedding. Encryption algorithms designed specifically for images can be used to maximize efficiency, such as chaos-based image ciphers. These encryption algorithms must fulfill both diffusion and confusion properties. Another important property that needs to be addressed is resistance against data loss or noise attacks.
2) Many chaos-based watermark encryption used classical chaotic maps such as the logistic map or the Arnold map. These type of maps are not secure enough as they have various security issues and periodic behaviour [173]–[175]. Cryptanalytic attacks can be performed to compromise encrypted watermarks. New or recently proposed chaotic maps can be used to support watermark encryption methods [176].
3) To improve security in hybrid SVD watermarking schemes, the secret key should be subjected to the cryptographic requirements. In most existing schemes, side information are used as secret keys. This can include SVD components, scale factors, digital signatures of the watermark image, MSF values, and the PRNG seeds that control the embedding blocks. Watermarking scheme can instead rely on conventional secret keys with a keyspace larger than 2^{128}, and the scheme should be highly sensitivity to small changes to the key (confusion property).
4) To achieve a good trade-off between robustness and imperceptibility, the optimal MSF values are identified

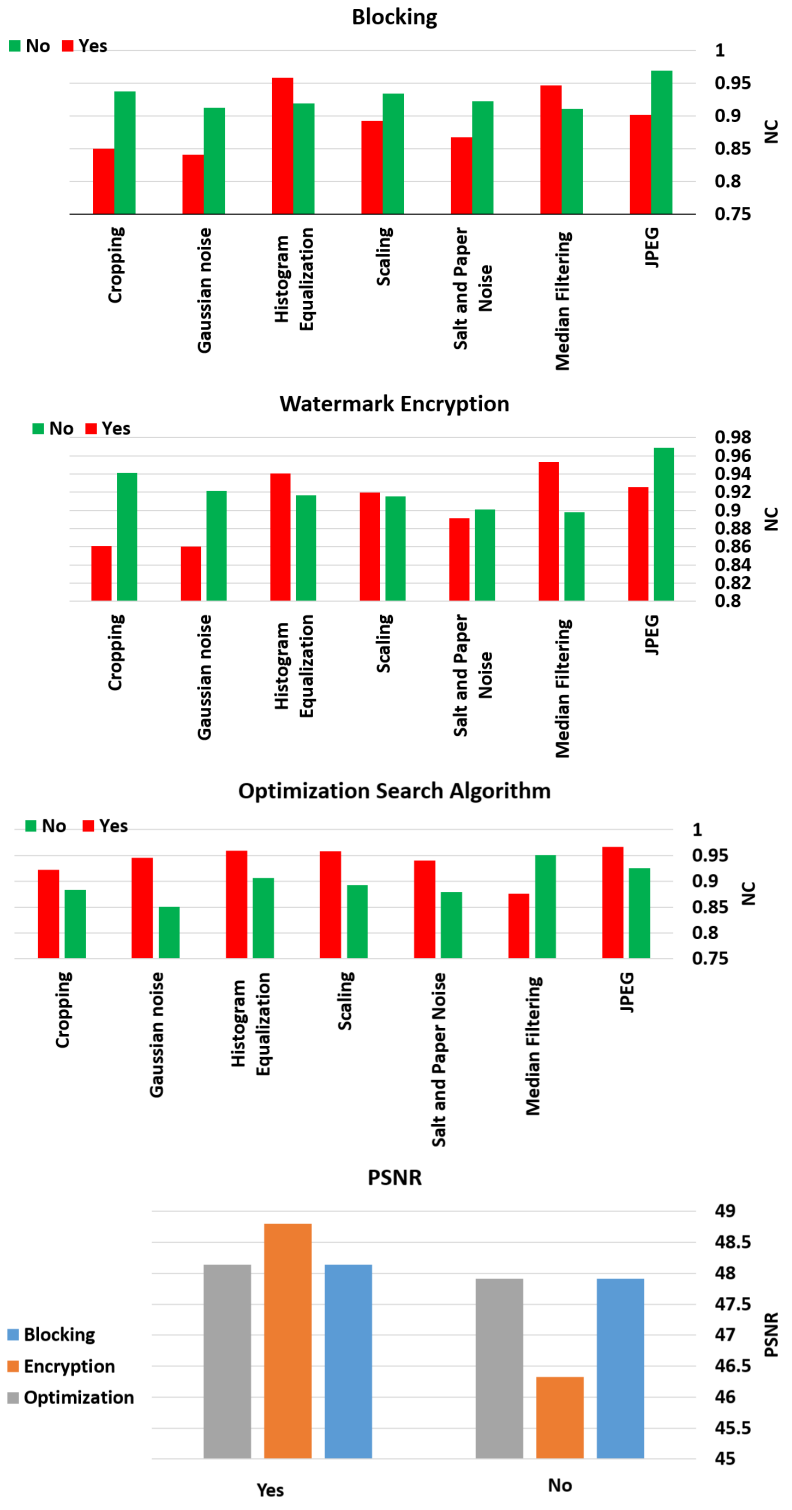

FIGURE 15. The average values of different attacks and PSNR for the existing schemes according to three strategies (blocking, optimization, and encryption).

by optimization algorithms such as ABC, DE, etc. Rather, PRNG and digital chaotic maps can be used to identify MSF values. This is not just more efficient but is highly flexible. MSF values based on random number generators do not incur significant computational overhead and the MSF values do not need to be preserved as a secret key for extraction.

TABLE 12. Imperceptibility and robustness results for the existing SVD-based watermarking schemes without used optimization search algorithms.

Scheme	PSNR	JPEG Compression	Median Filtering	Salt and Paper Noise	Re-Scaling	Histogram Equalization	Gaussian Noise	Cropping
[46]	22.21	0.996	0.995	0.994	0.983	-	-	-
[44]	48.09	-	0.9522	0.5903	0.9727	-	0.546	0.975
[121]	-	0.8772	1	0.997	0.9037	-	0.9579	0.9297
[159]	31.35	0.9886	0.9395	0.6883	-	-	0.8647	0.4266
[30]	64.35	-	-	-	-	-	-	-
[164]	35.84	0.9905	0.9982	0.7552	0.7375	0.569	0.7267	0.9829
[160]	50.52	0.9019	0.8019	0.8384	0.7926	0.953	0.9018	0.9845
[12]	36.69	0.9979	-	-	0.9866	-	0.9829	0.9972
[28]	58.03	-	0.9988	0.9998	-	-	0.9999	-
[146]	64.46	0.989	-	-	0.94	0.657	0.865	0.982
[29]	51.14	0.9226	-	-	-	0.97	0.9377	0.9377
[95]	43.3653	0.9824	0.7534	0.7515	0.5127	0.9648	0.7926	-
[65]	54.035DB	0.952	0.982	0.668	0.788	0.99	0.979	0.994
[113]	43.87	0.969	0.987	0.75	0.971	-	0.755	0.995
[112]	43.6769	0.9978	0.9707	0.995	0.984	0.985	0.589	0.9708
[161]	57.94	0.9717	0.9375	-	0.8076	0.9922	0.7988	0.9629
[148]	53.77	-	-	-	-	-	-	-
[152]	45.38	0.072	-	-	-	-	0.061	0.059
[130]	54.51	-	-	-	-	-	-	-
[129]	48.8	0.9941	0.9688	-	-	0.999	0.5928	0.8476
[144]	43.33	0.5057	0.6173	0.4986	0.4418	0.7962	0.4772	0.5996
[145]	-	0.9812	-	-	0.9	-	-	0.925
[151]	59.06	0.9931	0.9693	0.964	0.9879	0.9932	0.9215	0.9208
[131]	35.48	0.9901	0.9486	0.973	0.9952	-	-	0.954
[122]	67.45	-	0.9986	0.989	0.999	0.8805	0.9848	0.7473
[133]	39.39	0.9986	0.9812	0.9633	-	0.9984	0.9989	-
[13]	35.84	0.9905	0.9985	0.7552	0.8964	0.569	0.7267	-
[128]	-	0.998	-	-	-	-	-	0.9917
[139]	47.62	0.9882	0.9844	0.9504	-	-	0.9797	0.9567
[165]	47.48	-	0.983	0.9903	-	0.9953	0.9793	-
[140]	57.09	0.984	0.982	0.996	0.965	-	0.992	1
[166]	101.97	0.8569	0.9793	0.9988	0.9638	-	0.9985	-
[127]	-	0.9988	0.9949	-	0.9966	0.9827	0.9995	-
[167]	33.53	0.9934	0.9837	-	-	0.9726	0.9586	-
[153]	50.81	0.9945	0.9861	-	-	-	0.9896	0.9176
[154]	58.48	0.7401	0.9962	0.9859	0.9994		0.9591	0.9993
[157]	36.61	-	-	-	-	-	-	-
[119]	37.4	-	-	-	-	-	-	-
[155]	57.1	0.9843	0.9823	0.9847	0.9779		0.9855	0.8855
[158]	42	-	-	-	-	-	-	-
[25]	35.49	-	-	-	-	-	-	-
[89]		0.9949	0.9888	0.9513	0.9914		0.9743	0.7917
[90]	42.12	0.9056	0.899	0.8374	-	-	-	-
[22]		0.9955	0.8811	0.9396	0.964	0.9991	0.9063	0.991
[108]	51.14	0.9525	0.9805	0.9384	0.8938	0.9233	0.9207	0.9479
[109]	50.45	0.9596	0.9651	0.782	0.743	0.9355	0.8255	0.9496
[162]	55	-	-	-	-	-	-	-

(-) denotes that proposed scheme has no result.

TABLE 13. Imperceptibility and robustness results for the existing SVD-based watermarking schemes with used optimization search algorithms.

Scheme	PSNR	JPEG Compression	Median Filtering	Salt and Paper Noise	Re-Scaling	Histogram Equalization	Gaussian Noise	Cropping
[45]	38.023	0.9996	0.9989	0.997	-	0.9946	-	-
[134]	47.49	0.984	-	-	-	0.9984	0.9735	0.9948
[51]	50.3	1	0.9994	-	0.9998	0.9864	0.9998	0.9783
[26]	53.04	1	-	0.97	1	0.794	0.92	0.572
[27]	40.02	0.9574	0.9988	0.8104	0.9076	0.9982	0.983	0.9347
[19]	43.88	0.9733	0.0025	0.7974	0.9177	0.9404	0.9741	0.861
[172]	-	0.967	-	0.995	0.997	0.969	0.963	0.994
[150]	50.18	0.963	0.418	0.963	1	0.991	-	0.941
[135]	38.39	0.85	-	-	0.812	0.864	0.711	-
[125]	50.942	0.948	-	0.933	0.999	0.974	0.967	0.918
[126]	35.23	0.9948	0.9816	-	-	0.9789	0.9669	0.9648
[124]	33.28	0.955	0.9357	-	0.9047	0.9187	0.9438	0.9222
[147]	52.85	-	-	0.98	0.999	0.994	0.987	0.951
[24]	42.92	0.993	0.9974	0.9353	0.9687	0.9311	0.9003	0.9822
[84]	40.07	0.9195	0.9953	0.9695	-	0.9953	0.9335	0.9993
[156]	38.47	0.9592	0.9774	-	0.9851	-	0.9376	-
[98]	50.86	0.9307	0.9697	0.8701	0.832	0.997	-	0.8301
[137]	45.12	0.9996	0.9896	0.9989	0.9889	0.9878	0.9446	0.9884
[163]	59.26	0.9751	0.8917	0.9345	0.993	0.9074	0.9711	0.951
[168]	77.48	0.9945	0.9959	0.9554	0.9962	0.9725	0.9504	0.8922
[169]	74.99	-	0.99	0.995	0.995	0.991	0.9901	-

(-) denotes that proposed scheme has no result.

5) One or two frequency transforms should be used alongside SVD for the embedding phase to improve overall performance and imperceptibility.
6) A blocking strategy should be adopted to divide the host and the watermark images into non-overlapping blocks. Then, properties of these non-overlapping blocks can be leveraged for embedding, leading to lower distortions.
7) Another approach that can be investigated is to embed watermarks during host image creation. Though most image watermarking schemes use preexisting host images to embed the watermarks, the inclusion of watermark information during the host image creation process can be studied to enhance the security of the watermarking scheme [9].
8) The embedding capacity of an image watermarking scheme could be increased by repeating the same watermark information in all sub-bands of the host image. One can benefit from the repeat embedding in the host image to ensure better robustness in the extraction process.
9) Selecting a better frequency transform domain can also lead to improved schemes. Hybrid-based watermarking schemes depict improved results as compared to schemes that rely solely on the spatial domain. Thus, a watermark image should be converted to the frequency domain prior to the embedding process.
10) The design of a color watermarking scheme needs to consider different embedding sizes and strategies. Having multiple color channels leads to challenges during the embedding process due to the increased amount of information involved.
11) Embedding in singular values have better results in imperceptibility and robustness but leads to FPP. Thus, enhancement of SVD-based image watermarking schemes based on singular value embedding is still required.
12) Key management is vital for protecting watermarked image from future attacks and should be employed in newly proposed schemes.
13) MSF parameters need to be studied with respect to various attacks and different watermark sizes.

XI. CONCLUSION

Watermarking is one of the common strategies used to secure ownership and copyright. This paper has provided a detailed coverage of the state-of-the-art in image watermarking schemes based on SVD and hybrid frequency domains. In this paper, we have provided background information on watermarking such as watermark concepts, requirements, types, and frequency domain methods. Then, the paper shifts its focus to analyze existing hybrid SVD image watermarking schemes. The analysis includes SVD security issues (FPP attacks), hybrid SVD scheme classification, type of SVD embedding strategies, and comparison of SVD schemes. Performance comparison between existing schemes have revealed open security issues and research gaps such as FPP avoidance sans authentication steps, achieving good tradeoffs between robustness and imperceptibility without relying on optimal MSF parameters, and having a large embedding capacity while retaining high imperceptibility in the extraction phase. In future work, researchers can focus on developing hybrid SVD-based watermarking schemes for various applications that rely on medical or color images. A study on watermarking schemes for other media such as video is also still required. Performance comparisons and design recommendations provided in the paper can aid researchers or practitioners in developing or adopting watermarking schemes for various applications.

CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] A. K. Singh, "Some new techniques of improved wavelet domain watermarking OFR medical images," Ph.D. dissertation, Dept. Comput. Eng., NIT Kurukshetra, Haryana, India, 2015.
[2] P. Singh and R. S. Chadha, "A survey of digital watermarking techniques, applications and attacks," *Int. J. Eng. Innov. Technol.*, vol. 2, no. 9, pp. 165–175, 2013.
[3] C. Iwendi, Z. Jalil, A. R. Javed, T. Reddy G., R. Kaluri, G. Srivastava, and O. Jo, "KeySplitWatermark: Zero watermarking algorithm for software protection against cyber-attacks," *IEEE Access*, vol. 8, pp. 72650–72660, 2020.
[4] M. Taleby Ahvanooey, Q. Li, X. Zhu, M. Alazab, and J. Zhang, "ANiTW: A novel intelligent text watermarking technique for forensic identification of spurious information on social media," *Comput. Secur.*, vol. 90, Mar. 2020, Art. no. 101702.
[5] W. El-Shafai, S. El-Rabaie, M. M. El-Halawany, and F. E. A. El-Samie, "Security of 3D-HEVC transmission based on fusion and watermarking techniques," *Multimedia Tools Appl.*, vol. 78, no. 19, pp. 27211–27244, Oct. 2019.
[6] O. S. Faragallah, A. Afifi, H. S. El-Sayed, M. A. Alzain, J. F. Al-Amri, F. E. A. El-Samie, and W. El-Shafai, "Efficient HEVC integrity verification scheme for multimedia cybersecurity applications," *IEEE Access*, vol. 8, pp. 167069–167089, 2020.
[7] A. Khan, A. Siddiqa, S. Munib, and S. A. Malik, "A recent survey of reversible watermarking techniques," *Inf. Sci.*, vol. 279, pp. 251–272, Sep. 2014.
[8] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*. San Mateo, CA, USA: Morgan Kaufmann, 2007.
[9] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, no. 3, pp. 727–752, Mar. 2010.
[10] A. Zigomitros, A. Papageorgiou, and C. Patsakis, "Social network content management through watermarking," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 1381–1386.
[11] F. Bertini, R. Sharma, A. Iannì, and D. Montesi, "Smartphone verification and user profiles linking across social networks by camera fingerprinting," in *Proc. Int. Conf. Digit. Forensics Cyber Crime*. Cham, Switzerland: Springer, 2015, pp. 176–186.
[12] K. A. Al-Afandy, W. El-Shafai, E.-S.-M. El-Rabaie, F. E. Abd El-Samie, O. S. Faragallah, A. El-Mhalawy, A. M. Shehata, G. M. El-Banby, and M. M. El-Halawany, "Robust hybrid watermarking techniques for different color imaging systems," *Multimedia Tools Appl.*, vol. 77, no. 19, pp. 25709–25759, Oct. 2018.
[13] A. K. Singh, "Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images," *Multimedia Tools Appl.*, vol. 76, no. 6, pp. 8881–8900, Mar. 2017.
[14] C. Qin, X. Qian, W. Hong, and X. Zhang, "An efficient coding scheme for reversible data hiding in encrypted image with redundancy transfer," *Inf. Sci.*, vol. 487, pp. 176–192, Jun. 2019.
[15] K. Shankar and M. Elhoseny, "An optimal singular value decomposition with LWC-rectangle block cipher based digital image watermarking in wireless sensor networks," in *Secure Image Transmission in Wireless Sensor Network (WSN) Applications*. Cham, Switzerland: Springer, 2019, pp. 83–98.
[16] D. Xu and S. Su, "Separable reversible data hiding in encrypted images based on difference histogram modification," *Secur. Commun. Netw.*, vol. 2019, pp. 1–14, Jun. 2019.
[17] L. Chen, J. Chen, G. Zhao, and S. Wang, "Cryptanalysis and improvement of a chaos-based watermarking scheme," *IEEE Access*, vol. 7, pp. 97549–97565, 2019.
[18] N. M. Makbol, B. E. Khoo, and T. H. Rassem, "Security analyses of false positive problem for the SVD-based hybrid digital image watermarking techniques in the wavelet transform domain," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 26845–26879, Oct. 2018.
[19] A. Zear, A. K. Singh, and P. Kumar, "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine," *Multimedia Tools Appl.*, vol. 77, no. 4, pp. 4863–4882, Feb. 2018.
[20] L. Rosales-Roldan, J. Chao, M. Nakano-Miyatake, and H. Perez-Meana, "Color image ownership protection based on spectral domain watermarking using QR codes and QIM," *Multimedia Tools Appl.*, vol. 77, no. 13, pp. 16031–16052, Jul. 2018.
[21] F. A. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in *Proc. Int. Workshop Inf. Hiding*. Cham, Switzerland: Springer, 1998, pp. 218–238.
[22] J. Li, C. Yu, B. B. Gupta, and X. Ren, "Color image watermarking scheme based on quaternion Hadamard transform and schur decomposition," *Multimedia Tools Appl.*, vol. 77, no. 4, pp. 4545–4561, Feb. 2018.
[23] Z. Yuan, Q. Su, D. Liu, and X. Zhang, "A blind image watermarking scheme combining spatial domain and frequency domain," *Vis. Comput.*, pp. 1–15, Jul. 2020.
[24] N. M. Makbol, B. E. Khoo, T. H. Rassem, and K. Loukhaoukha, "A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection," *Inf. Sci.*, vol. 417, pp. 381–400, Nov. 2017.
[25] K. Chaitanya, E. S. Reddy, and K. G. Rao, "Digital color image watermarking in RGB planes using DWT-DCT-SVD coefficients," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 2, pp. 2413–2417, 2014.
[26] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, "Optimized gray-scale image watermarking using DWT–SVD and firefly algorithm," *Expert Syst. Appl.*, vol. 41, no. 17, pp. 7858–7867, Dec. 2014.
[27] M. Ali, C. W. Ahn, M. Pant, and P. Siarry, "An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony," *Inf. Sci.*, vol. 301, pp. 44–60, Apr. 2015.
[28] I. Assini, A. Badri, K. Safi, A. Sahel, and A. Baghdad, "A robust hybrid watermarking technique for securing medical image," *Int. J. Intell. Eng. Syst.*, vol. 11, no. 3, pp. 169–176, Jun. 2018.
[29] C.-C. Lai and C.-C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 11, pp. 3060–3063, Nov. 2010.
[30] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial Internet of Things (IIoT)–enabled framework for health monitoring," *Comput. Netw.*, vol. 101, pp. 192–202, Jun. 2016.
[31] S. N. Prajwalasimha, H. Swapna, and A. Shetter, "Digital image watermarking based on sine transformation with constant co-efficient," in *Proc. Int. Conf. Inventive Res. Comput. Appl. (ICIRCA)*, Jul. 2018, pp. 21–24.
[32] R. K. Senapati, S. Srivastava, and P. Mankar, "RST invariant blind image watermarking schemes based on discrete tchebichef transform and singular value decomposition," *Arabian J. Sci. Eng.*, vol. 45, pp. 3331–3353, 2020.
[33] E. Elbasi, "M-SVD based quality measurement in hybrid non-blind watermarked medical images," in *Proc. 43rd Int. Conf. Telecommun. Signal Process. (TSP)*, Jul. 2020, pp. 506–510.
[34] R. Artru, A. Gouaillard, and T. Ebrahimi, "Digital watermarking of video streams: Review of the state-of-the-art," 2019, *arXiv:1908.02039*. [Online]. Available: http://arxiv.org/abs/1908.02039
[35] K. Meenakshi, K. Swaraja, and P. Kora, "A robust DCT-SVD based video watermarking using zigzag scanning," in *Soft Computing and Signal Processing*. Cham, Switzerland: Springer, 2019, pp. 477–485.
[36] S. Kumar, B. K. Singh, and M. Yadav, "A recent survey on multimedia and database watermarking," *Multimedia Tools Appl.*, vol. 79, pp. 20149–20197, Jul. 2020.
[37] O. P. Singh, A. K. Singh, G. Srivastava, and N. Kumar, "Image watermarking using soft computing techniques: A comprehensive survey," *Multimedia Tools Appl.*, pp. 1–32, Aug. 2020.
[38] O. Evsutin, A. Melman, and R. Meshcheryakov, "Digital steganography and watermarking for digital images: A review of current research directions," *IEEE Access*, vol. 8, pp. 166589–166611, 2020.
[39] C. Kumar, A. K. Singh, and P. Kumar, "A recent survey on image watermarking techniques and its application in e-governance," *Multimedia Tools Appl.*, vol. 77, no. 3, pp. 3597–3622, Feb. 2018.
[40] L. Singh, A. Singh, and P. Singh, "Secure data hiding techniques: A survey," *Multimedia Tools Appl.*, vol. 79, pp. 15901–15921, Jun. 2020.
[41] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, "Watermarking techniques used in medical images: A survey," *J. Digit. Imag.*, vol. 27, no. 6, pp. 714–729, Dec. 2014.
[42] N. Agarwal, A. K. Singh, and P. K. Singh, "Survey of robust and imperceptible watermarking," *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 8603–8633, Apr. 2019.

[43] N. V. Dharwadkar, B. B. Amberker, and A. Gorai, "Non-blind watermarking scheme for color images in RGB space using DWT-SVD," in *Proc. Int. Conf. Commun. Signal Process.*, Feb. 2011, pp. 489–493.

[44] N. El-Houda Golea, R. Seghir, and R. Benzid, "A bind RGB color image watermarking based on singular value decomposition," in *Proc. ACS/IEEE Int. Conf. Comput. Syst. Appl. (AICCSA)*, May 2010, pp. 1–5.

[45] V. Aslantas, "An optimal robust digital image watermarking based on SVD using differential evolution algorithm," *Opt. Commun.*, vol. 282, no. 5, pp. 769–777, Mar. 2009.

[46] M.-S. Wang and W.-C. Chen, "A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography," *Comput. Standards Interfaces*, vol. 31, no. 4, pp. 757–762, Jun. 2009.

[47] S. B. B. Ahmadi, G. Zhang, and S. Wei, "Robust and hybrid SVD-based image watermarking schemes," *Multimedia Tools Appl.*, vol. 79, pp. 1075–1117, Jan. 2020.

[48] P. Meerwald and A. Uhl, "Survey of wavelet-domain watermarking algorithms," *Proc. SPIE*, vol. 4314, pp. 505–516, Aug. 2001.

[49] S. Oueslati and B. Solaiman, "Watermarking medical images with patient identification to verify authenticity," *Int. J. Med. Eng. Informat.*, vol. 10, no. 1, pp. 86–101, 2018.

[50] M. Arsalan, A. S. Qureshi, A. Khan, and M. Rajarajan, "Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique," *Appl. Soft Comput.*, vol. 51, pp. 168–179, Feb. 2017.

[51] M. Ali, C. W. Ahn, and M. Pant, "A robust image watermarking technique using SVD and differential evolution in DCT domain," *Optik*, vol. 125, no. 1, pp. 428–434, Jan. 2014.

[52] R. B. Wolfgang and E. J. Delp, "A watermark for digital images," in *Proc. 3rd IEEE Int. Conf. Image Process.*, vol. 3, Sep. 1996, pp. 219–222.

[53] R. Kaluri, V. University, P. Ch, and V. University, "An enhanced framework for sign gesture recognition using hidden Markov model and adaptive histogram technique," *Int. J. Intell. Eng. Syst.*, vol. 10, no. 3, pp. 11–19, Jun. 2017.

[54] A. K. Singh, B. Kumar, M. Dave, S. P. Ghrera, and A. Mohan, "Digital image watermarking: Techniques and emerging applications," in *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*. Hershey, PA, USA: IGI Global, 2016, pp. 246–272.

[55] A. K. Singh, B. Kumar, G. Singh, and A. Mohan, *Medical Image Watermarking: Techniques and Applications*. Cham, Switzerland: Springer, 2017.

[56] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *IEEE Signal Process. Mag.*, vol. 17, no. 5, pp. 20–46, 2000.

[57] P. Wayner, *Disappearing Cryptography: Information Hiding: Steganography & Watermarking*. San Mateo, CA, USA: Morgan Kaufmann, 2009.

[58] H. Nyeem, W. Boles, and C. Boyd, "A review of medical image watermarking requirements for teleradiology," *J. Digit. Imag.*, vol. 26, no. 2, pp. 326–343, Apr. 2013.

[59] J. Sang and M. S. Alam, "Fragility and robustness of binary-phase-only-filter-based fragile/semifragile digital image watermarking," *IEEE Trans. Instrum. Meas.*, vol. 57, no. 3, pp. 595–606, Mar. 2008.

[60] U. Gokhale and Y. Joshi, "A semi fragile watermarking algorithm based on SVD-IWT for image authentication," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 1, no. 4, pp. 217–222, 2012.

[61] Z. Wenyin and F. Y. Shih, "Semi-fragile spatial watermarking based on local binary pattern operators," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3904–3912, Aug. 2011.

[62] J.-D. Chang, B.-H. Chen, and C.-S. Tsai, "LBP-based fragile watermarking scheme for image tamper detection and recovery," in *Proc. Int. Symp. Next-Gener. Electron.*, Feb. 2013, pp. 173–176.

[63] A. Piva, "An overview on image forensics," *ISRN Signal Process.*, vol. 2013, pp. 1–22, Jan. 2013.

[64] G. Zhou and D. Lv, "An overview of digital watermarking in image forensics," in *Proc. 4th Int. Joint Conf. Comput. Sci. Optim.*, Apr. 2011, pp. 332–335.

[65] N. M. Makbol and B. E. Khoo, "Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition," *AEU-Int. J. Electron. Commun.*, vol. 67, no. 2, pp. 102–112, Feb. 2013.

[66] H. Shi and F. Lv, "A blind digital watermark technique for color image based on integer wavelet transform," in *Proc. Int. Conf. Biomed. Eng. Comput. Sci.*, Apr. 2010, pp. 1–4.

[67] C.-C. Chang, C.-C. Lin, C.-S. Tseng, and W.-L. Tai, "Reversible hiding in DCT-based compressed images," *Inf. Sci.*, vol. 177, no. 13, pp. 2768–2786, Jul. 2007.

[68] S. Zaboli and M. S. Moin, "CEW: A non-blind adaptive image watermarking approach based on entropy in contourlet domain," in *Proc. IEEE Int. Symp. Ind. Electron.*, Jun. 2007, pp. 1687–1692.

[69] R. Ni, Q. Ruan, and H. D. Cheng, "Secure semi-blind watermarking based on iteration mapping and image features," *Pattern Recognit.*, vol. 38, no. 3, pp. 357–368, Mar. 2005.

[70] E. F. Badran, M. A. Sharkas, and O. A. Attallah, "Multiple watermark embedding scheme in wavelet-spatial domains based on roi of medical images," in *Proc. Nat. Radio Sci. Conf.*, Mar. 2009, pp. 1–8.

[71] T. Agung B. W. Adiwijaya, and F. P. Permana, "Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and run length encoding (RLE) compression," in *Proc. IEEE Int. Conf. Commun., Netw. Satell. (ComNetSat)*, Jul. 2012, pp. 167–171.

[72] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Trans. Image Process.*, vol. 14, no. 2, pp. 253–266, Feb. 2005.

[73] H. Zhang, C. Wang, and X. Zhou, "Fragile watermarking based on LBP for blind tamper detection in images," *J. Inf. Process. Syst.*, vol. 13, no. 2, pp. 385–399, 2017.

[74] S. Rahman, C. Saha, M. F. Hossain, and T. A. Tamal, "Integer wavelet transform based dual watermarking technique using tent map and local binary pattern," *Global J. Res. Eng.*, vol. 18, no. 3-F, 2018.

[75] T. Ahonen, A. Hadid, and M. Pietikäinen, "Face recognition with local binary patterns," in *Proc. Eur. Conf. Comput. Vis.* Cham, Switzerland: Springer, 2004, pp. 469–481.

[76] S. Nigam, R. Singh, and A. Misra, "Local binary patterns based facial expression recognition for efficient smart applications," in *Security in Smart Cities: Models, Applications, and Challenges*. Cham, Switzerland: Springer, 2019, pp. 297–322.

[77] R. Javid, M. M. Riaz, A. Ghafoor, and N. Iqbal Rao, "Direction, velocity, merging probabilities and shape descriptors for crowd behavior analysis," *IEEE Access*, vol. 7, pp. 102561–102568, 2019.

[78] E. Chrysochos, V. Fotopoulos, M. Xenos, and A. N. Skodras, "Hybrid watermarking based on chaos and histogram modification," *Signal, Image Video Process.*, vol. 8, no. 5, pp. 843–857, Jul. 2014.

[79] V. Kelkar, K. Tuckley, and H. Nemade, "Novel variants of a histogram shift-based reversible watermarking technique for medical images to improve hiding capacity," *J. Healthcare Eng.*, vol. 2017, pp. 1–7, Jan. 2017.

[80] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[81] M. R. Khosravi and M. Yazdi, "A lossless data hiding scheme for medical images using a hybrid solution based on IBRW error histogram computation and quartered interpolation with greedy weights," *Neural Comput. Appl.*, vol. 30, no. 7, pp. 2017–2028, Oct. 2018.

[82] T. K. Tewari and V. Saxena, "An improved and robust DCT based digital image watermarking scheme," *Int. J. Comput. Appl.*, vol. 3, no. 1, pp. 28–32, Jun. 2010.

[83] L.-Y. Hsu and H.-T. Hu, "Robust blind image watermarking using crisscross inter-block prediction in the DCT domain," *J. Vis. Commun. Image Represent.*, vol. 46, pp. 33–47, Jul. 2017.

[84] X.-B. Kang, F. Zhao, G.-F. Lin, and Y.-J. Chen, "A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength," *Multimedia Tools Appl.*, vol. 77, no. 11, pp. 13197–13224, Jun. 2018.

[85] J. Mohamad Zain and M. Clarke, "Reversible region of non-interest (RONI) watermarking for authentication of DICOM images," 2011, *arXiv:1101.1603*. [Online]. Available: http://arxiv.org/abs/1101.1603

[86] S. A. Parah, J. A. Sheikh, N. A. Loan, and G. M. Bhat, "Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing," *Digit. Signal Process.*, vol. 53, pp. 11–24, Jun. 2016.

[87] S. Liu, Z. Pan, and H. Song, "Digital image watermarking method based on DCT and fractal encoding," *IET Image Process.*, vol. 11, no. 10, pp. 815–821, Oct. 2017.

[88] R. A. Alotaibi and L. A. Elrefaei, "Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT)," *Appl. Comput. Informat.*, vol. 15, no. 2, pp. 191–202, Jul. 2019.

[89] X. Wu and W. Sun, "Robust copyright protection scheme for digital images using overlapping DCT and SVD," *Appl. Soft Comput.*, vol. 13, no. 2, pp. 1170–1182, Feb. 2013.
[90] C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, "Robust and imperceptible image watermarking by DC coefficients using singular value decomposition," in *Proc. 4th Int. Conf. Electr. Eng., Comput. Sci. Informat. (EECSI)*, Sep. 2017, pp. 1–5.
[91] R. Gill and R. Soni, "An efficient image watermarking using 2-DCT AND 2-DWT in color images," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 5, pp. 1304–1308, 2017.
[92] G. S. Kalra, R. Talwar, and H. Sadawarti, "Adaptive digital image watermarking for color images in frequency domain," *Multimedia Tools Appl.*, vol. 74, no. 17, pp. 6849–6869, Sep. 2015.
[93] S. Roy and A. K. Pal, "A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling," *Multimedia Tools Appl.*, vol. 76, no. 3, pp. 3577–3616, Feb. 2017.
[94] N. Kashyap and G. Sinha, "Image watermarking using 3-level discrete wavelet transform (DWT)," *Int. J. Mod. Educ. Comput. Sci.*, vol. 4, no. 3, p. 50, 2012.
[95] S. Rastegar, F. Namazi, K. Yaghmaie, and A. Aliabadian, "Hybrid watermarking algorithm based on singular value decomposition and radon transform," *AEU-Int. J. Electron. Commun.*, vol. 65, no. 7, pp. 658–663, Jul. 2011.
[96] B. L. Gunjal and S. N. Mali, "Roi based embedded watermarking of medical images for secured communication in telemedicine," *Int. J. Comput. Commun. Eng.*, vol. 6, no. 48, pp. 293–298, 2012.
[97] B. Hemamalini and V. Nagarajan, "Wavelet transform and pixel strength-based robust watermarking using dragonflyoptimization," *Multimedia Tools Appl.*, vol. 79, pp. 8727–8746, Apr. 2020.
[98] E. Moeinaddini and F. Afsari, "Robust watermarking in DWT domain using SVD and opposition and dimensional based modified firefly algorithm," *Multimedia Tools Appl.*, vol. 77, no. 19, pp. 26083–26105, Oct. 2018.
[99] A. Ahmad, G. Sinha, and N. Kashyap, "3-level DWT image watermarking against frequency and geometrical attacks," *Int. J. Comput. Netw. Inf. Secur.*, vol. 6, no. 12, p. 58, 2014.
[100] B. Yadav, A. Kumar, and Y. Kumar, "A robust digital image watermarking algorithm using DWT and SVD," in *Soft Computing: Theories and Applications*. Cham, Switzerland: Springer, 2018, pp. 25–36.
[101] H. Gao, L. Jia, and M. Liu, "A digital watermarking algorithm for color image based on DWT," *TELKOMNIKA Indonesian J. Electr. Eng.*, vol. 11, no. 6, pp. 3271–3278, Jun. 2013.
[102] K. J. Giri, M. A. Peer, and P. Nagabhushan, "A robust color image watermarking scheme using discrete wavelet transformation," *Int. J. Image, Graph. Signal Process.*, vol. 7, no. 1, pp. 47–52, Dec. 2014.
[103] M. Gupta, G. Parmar, R. Gupta, and M. Saraswat, "Discrete wavelet transform-based color image watermarking using uncorrelated color space and artificial bee colony," *Int. J. Comput. Intell. Syst.*, vol. 8, no. 2, pp. 364–380, Mar. 2015.
[104] T. Huynh-The, C.-H. Hua, N. A. Tu, T. Hur, J. Bang, D. Kim, M. B. Amin, B. Ho Kang, H. Seung, and S. Lee, "Selective bit embedding scheme for robust blind color image watermarking," *Inf. Sci.*, vol. 426, pp. 1–18, Feb. 2018.
[105] P. Rasti, G. Anbarjafari, and H. Demirel, "Colour image watermarking based on wavelet and QR decomposition," in *Proc. 25th Signal Process. Commun. Appl. Conf. (SIU)*, May 2017, pp. 1–4.
[106] A. Roy, A. K. Maiti, and K. Ghosh, "An HVS inspired robust non-blind watermarking scheme in YCbCr color space," *Int. J. Image Graph.*, vol. 18, no. 3, Jul. 2018, Art. no. 1850015.
[107] Y. Lakrissi, A. Saaidi, and A. Essahlaoui, "Novel dynamic color image watermarking based on DWT-SVD and the human visual system," *Multimedia Tools Appl.*, vol. 77, no. 11, pp. 13531–13555, Jun. 2018.
[108] S. Roy and A. K. Pal, "A hybrid domain color image watermarking based on DWT–SVD," *Iranian J. Sci. Technol., Trans. Elect. Eng.*, vol. 43, no. 2, pp. 201–217, Jun. 2019.
[109] S. Roy and A. K. Pal, "An SVD based location specific robust color image watermarking scheme using RDWT and arnold scrambling," *Wireless Pers. Commun.*, vol. 98, no. 2, pp. 2223–2250, Jan. 2018.
[110] R. Thanki and S. Borra, "A color image steganography in hybrid FRT–DWT domain," *J. Inf. Secur. Appl.*, vol. 40, pp. 92–102, Jun. 2018.
[111] L. Fan, T. Gao, and Q. Yang, "A novel zero-watermark copyright authentication scheme based on lifting wavelet and harris corner detection," *Wuhan Univ. J. Natural Sci.*, vol. 15, no. 5, pp. 408–414, Oct. 2010.
[112] N. M. Makbol and B. E. Khoo, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition," *Digit. Signal Process.*, vol. 33, pp. 134–147, Oct. 2014.
[113] N. M. Makbol and B. E. Khoo, "A hybrid robust image watermarking scheme using integer wavelet transform, singular value decomposition and Arnold transform," in *Proc. Int. Vis. Informat. Conf.* Cham, Switzerland: Springer, 2013, pp. 36–47.
[114] B. Wang, "Reversible integer wavelet transform for the joint of image encryption and watermarking," *Math. Problems Eng.*, vol. 2015, pp. 1–11, Jan. 2015.
[115] B. Zhou and J. Chen, "A geometric distortion resilient image watermarking algorithm based on SVD," *J. Image Graph.*, vol. 4, pp. 506–512, Apr. 2004.
[116] S. B. B. Ahmadi, G. Zhang, M. Rabbani, L. Boukela, and H. Jelodar, "An intelligent and blind dual color image watermarking for authentication and copyright protection," *Appl. Intell.*, vol. 51, pp. 1701–1732, 2021.
[117] N. A. Memon, A. Chaudhry, M. Ahmad, and Z. A. Keerio, "Hybrid watermarking of medical images for ROI authentication and recovery," *Int. J. Comput. Math.*, vol. 88, no. 10, pp. 2057–2071, Jul. 2011.
[118] N. A. Memon and S. A. M. Gilani, "Watermarking of chest CT scan medical images for content authentication," *Int. J. Comput. Math.*, vol. 88, no. 2, pp. 265–280, Jan. 2011.
[119] R. A. Sadek, "SVD based image processing applications: State of the art, contributions and research challenges," 2012, *arXiv:1211.7102*. [Online]. Available: http://arxiv.org/abs/1211.7102
[120] Q. Li, C. Yuan, and Y.-Z. Zhong, "Adaptive DWT-SVD domain image watermarking using human visual model," in *Proc. 9th Int. Conf. Adv. Commun. Technol.*, vol. 3, Feb. 2007, pp. 1947–1951.
[121] S.-L. Jia, "A novel blind color images watermarking based on SVD," *Optik*, vol. 125, no. 12, pp. 2868–2874, Jun. 2014.
[122] T. K. Araghi, A. A. Manaf, and S. K. Araghi, "A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition," *Expert Syst. Appl.*, vol. 112, pp. 208–228, Dec. 2018.
[123] C. Jain, S. Arora, and P. K. Panigrahi, "A reliable SVD based watermarking schem," 2008, *arXiv:0808.0309*. [Online]. Available: http://arxiv.org/abs/0808.0309
[124] M. Ali and C. W. Ahn, "An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain," *Signal Process.*, vol. 94, pp. 545–556, Jan. 2014.
[125] K. Loukhaoukha, "Image watermarking algorithm based on multiobjective ant colony optimization and singular value decomposition in wavelet domain," *J. Optim.*, vol. 2013, pp. 1–10, Jun. 2013.
[126] M. Ali, C. W. Ahn, and P. Siarry, "Differential evolution algorithm for the selection of optimal scaling factors in image watermarking," *Eng. Appl. Artif. Intell.*, vol. 31, pp. 15–26, May 2014.
[127] M. Ali, C. W. Ahn, and M. Pant, "An efficient lossless robust watermarking scheme by integrating redistributed invariant wavelet and fractional Fourier transforms," *Multimedia Tools Appl.*, vol. 77, no. 10, pp. 11751–11773, May 2018.
[128] T. Amiri and M. E. Moghaddam, "A new visual cryptography based watermarking scheme using DWT and SIFT for multiple cover images," *Multimedia Tools Appl.*, vol. 75, no. 14, pp. 8527–8543, Jul. 2016.
[129] C.-C. Lai, "An improved SVD-based watermarking scheme using human visual characteristics," *Opt. Commun.*, vol. 284, no. 4, pp. 938–944, Feb. 2011.
[130] M.-Q. Fan, H.-X. Wang, and S.-K. Li, "Restudy on SVD-based watermarking scheme," *Appl. Math. Comput.*, vol. 203, no. 2, pp. 926–930, Sep. 2008.
[131] F. Zhang, T. Luo, G. Jiang, M. Yu, H. Xu, and W. Zhou, "A novel robust color image watermarking method using RGB correlations," *Multimedia Tools Appl.*, vol. 78, pp. 20133–20155, Jul. 2019.
[132] Q. Su, Y. Niu, H. Zou, Y. Zhao, and T. Yao, "A blind double color image watermarking algorithm based on QR decomposition," *Multimedia Tools Appl.*, vol. 72, no. 1, pp. 987–1009, Sep. 2014.
[133] S. Thakur, A. Singh, S. Ghrera, and A. Mohan, "Chaotic based secure watermarking approach for medical images," *Multimedia Tools Appl.*, vol. 79, no. 7, pp. 4263–4276, 2020.
[134] C.-C. Lai, "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm," *Digit. Signal Process.*, vol. 21, no. 4, pp. 522–527, Jul. 2011.
[135] R.-S. Run, S.-J. Horng, J.-L. Lai, T.-W. Kao, and R.-J. Chen, "An improved SVD-based watermarking technique for copyright protection," *Expert Syst. Appl.*, vol. 39, no. 1, pp. 673–689, Jan. 2012.

[136] J. Liu, J. Li, J. Ma, N. Sadiq, U. Bhatti, and Y. Ai, "A robust multi-watermarking algorithm for medical images based on DTCWT-DCT and henon map," *Appl. Sci.*, vol. 9, no. 4, p. 700, Feb. 2019.

[137] I. A. Ansari, M. Pant, and C. W. Ahn, "Robust and false positive free watermarking in IWT domain using SVD and ABC," *Eng. Appl. Artif. Intell.*, vol. 49, pp. 114–125, Mar. 2016.

[138] J. Bahi, C. Guyeux, and Q. Wang, "A novel pseudo-random generator based on discrete chaotic iterations," *Internet*, vol. 9, pp. 71–76, 2009.

[139] Z. Zhang, C. Wang, and X. Zhou, "Image watermarking scheme based on Arnold transform and DWT-DCT-SVD," in *Proc. IEEE 13th Int. Conf. Signal Process. (ICSP)*, Nov. 2016, pp. 805–810.

[140] S. Fazli and M. Moeini, "A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks," *Optik*, vol. 127, no. 2, pp. 964–972, Jan. 2016.

[141] S. S. Jamal, T. Shah, and I. Hussain, "An efficient scheme for digital watermarking using chaotic map," *Nonlinear Dyn.*, vol. 73, no. 3, pp. 1469–1474, Aug. 2013.

[142] M. Ghebleh, A. Kanso, and H. S. Own, "A blind chaos-based watermarking technique," *Secur. Commun. Netw.*, vol. 7, no. 4, pp. 800–811, Apr. 2014.

[143] A. Mooney, J. G. Keating, and I. Pitas, "A comparative study of chaotic and white noise signals in digital watermarking," *Chaos, Solitons Fractals*, vol. 35, no. 5, pp. 913–921, Mar. 2008.

[144] A. K. Gupta and M. S. Raval, "A robust and secure watermarking scheme based on singular values replacement," *Sadhana*, vol. 37, no. 4, pp. 425–440, Aug. 2012.

[145] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimedia*, vol. 4, no. 1, pp. 121–128, Mar. 2002.

[146] E. Ganic, "Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition," *J. Electron. Imag.*, vol. 14, no. 4, Oct. 2005, Art. no. 043004.

[147] K. Loukhaoukha, M. Nabti, and K. Zebbiche, "A robust SVD-based image watermarking using a multi-objective particle swarm optimization," *Opto-Electron. Rev.*, vol. 22, no. 1, pp. 45–54, Jan. 2014.

[148] J.-M. Guo and H. Prasetyo, "Security analyses of the watermarking scheme based on redundant discrete wavelet transform and singular value decomposition," *AEU-Int. J. Electron. Commun.*, vol. 68, no. 9, pp. 816–834, Sep. 2014.

[149] K. Loukhaoukha and J.-Y. Chouinard, "Hybrid watermarking algorithm based on SVD and lifting wavelet transform for ownership verification," in *Proc. 11th Can. Workshop Inf. Theory*, May 2009, pp. 177–182.

[150] K. Loukhaoukha, J.-Y. Chouinard, and M. H. Taieb, "Optimal image watermarking algorithm based on LWT-SVD via multi-objective ant colony optimization," *J. Inf. Hiding Multimedia Signal Process.*, vol. 2, no. 4, pp. 303–319, 2011.

[151] E. Najafi and K. Loukhaoukha, "Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform," *J. Inf. Secur. Appl.*, vol. 44, pp. 144–156, Feb. 2019.

[152] K.-L. Chung, W.-N. Yang, Y.-H. Huang, S.-T. Wu, and Y.-C. Hsu, "On SVD-based watermarking algorithm," *Appl. Math. Comput.*, vol. 188, no. 1, pp. 54–57, 2007.

[153] Y. Niu, X. Cui, Q. Li, and J. Ding, "A SVD-based color image watermark algorithm in DWT domain," in *Advanced Graphic Communications, Packaging Technology and Materials*. Cham, Switzerland: Springer, 2016, pp. 303–309.

[154] S. Ojha, A. Sharma, and R. Chaturvedi, "Centric-oriented novel image watermarking technique based on DWT and SVD," in *Soft Computing: Theories and Applications*. Cham, Switzerland: Springer, 2018, pp. 217–225.

[155] K.-F. He, J. Gao, L.-M. Hu, and H.-Y. Gao, "Watermarking for images using the HVS and SVD in the wavelet domain," in *Proc. Int. Conf. Mechatronics Autom.*, Jun. 2006, pp. 2352–2356.

[156] I. A. Ansari and M. Pant, "Multipurpose image watermarking in the domain of DWT based on SVD and ABC," *Pattern Recognit. Lett.*, vol. 94, pp. 228–236, Jul. 2017.

[157] V. Santhi and A. Thangavelu, "DWT-SVD combined full band robust watermarking technique for color images in YUV color space," *Int. J. Comput. Theory Eng.*, vol. 1, no. 4, p. 424, 2009.

[158] R. Buse Dili and E. Mwangi, "An image watermarking method based on the singular value decomposition and the wavelet transform," in *Proc. AFRICON*, Sep. 2007, pp. 1–5.

[159] J.-M. Guo and H. Prasetyo, "False-positive-free SVD-based image watermarking," *J. Vis. Commun. Image Represent.*, vol. 25, no. 5, pp. 1149–1163, Jul. 2014.

[160] S. Roy and A. K. Pal, "An indirect watermark hiding in discrete cosine transform–singular value decomposition domain for copyright protection," *Roy. Soc. Open Sci.*, vol. 4, no. 6, Jun. 2017, Art. no. 170326.

[161] N. M. Makbol, B. E. Khoo, and T. H. Rassem, "Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics," *IET Image Process.*, vol. 10, no. 1, pp. 34–52, Jan. 2016.

[162] K. Balasamy and S. Suganyadevi, "A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD," *Multimedia Tools Appl.*, pp. 1–20, Oct. 2020.

[163] M. Bansal, A. Mishra, and A. Sharma, "Optimized DWT SVD based image watermarking scheme using particle swarm optimization," in *Proc. Int. Conf. Comput. Sci. Appl.* Cham, Switzerland: Springer, Mar. 2012, pp. 862–877.

[164] A. K. Singh, M. Dave, and A. Mohan, "Hybrid technique for robust and imperceptible multiple watermarking using medical images," *Multimedia Tools Appl.*, vol. 75, no. 14, pp. 8381–8401, Jul. 2016.

[165] S. Arumugham, S. Rajagopalan, J. B. B. Rayappan, and R. Amirtharajan, "Tamper-resistant secure medical image carrier: An IWT–SVD–Chaos–FPGA combination," *Arabian J. Sci. Eng.*, vol. 44, pp. 9561–9580, Nov. 2019.

[166] X. Zhou, H. Zhang, and C. Wang, "A robust image watermarking technique based on DWT, APDCBT, and SVD," *Symmetry*, vol. 10, no. 3, p. 77, Mar. 2018.

[167] S. Rawat and B. Raman, "A blind watermarking algorithm based on fractional Fourier transform and visual cryptography," *Signal Process.*, vol. 92, no. 6, pp. 1480–1491, Jun. 2012.

[168] S. Sharma, H. Sharma, and J. B. Sharma, "An adaptive color image watermarking using RDWT-SVD and artificial bee colony based quality metric strength factor optimization," *Appl. Soft Comput.*, vol. 84, Nov. 2019, Art. no. 105696.

[169] B. Dappuri, M. P. Rao, and M. B. Sikha, "Non-blind RGB watermarking approach using SVD in translation invariant wavelet space with enhanced grey-wolf optimizer," *Multimedia Tools Appl.*, vol. 79, nos. 41–42, pp. 31103–31124, Nov. 2020.

[170] U. Rajendra Acharya, D. Acharya, P. Subbanna Bhat, and U. C. Niranjan, "Compact storage of medical images with patient information," *IEEE Trans. Inf. Technol. Biomed.*, vol. 5, no. 4, pp. 320–323, Dec. 2001.

[171] S. Lagzian, M. Soryani, and M. Fathy, "Robust watermarking scheme based on RDWT-SVD: Embedding data in all subbands," in *Proc. Int. Symp. Artif. Intell. Signal Process. (AISP)*, Jun. 2011, pp. 48–52.

[172] K. Loukhaoukha, J.-Y. Chouinard, and M. H. Taieb, "Multi-objective genetic algorithm optimization for image watermarking based on singular value decomposition and lifting wavelet transform," in *Proc. Int. Conf. Image Signal Process.* Cham, Switzerland: Springer, 2010, pp. 394–403.

[173] M. Alawida, A. Samsudin, J. S. Teh, and W. H. Alshoura, "Digital cosine chaotic map for cryptographic applications," *IEEE Access*, vol. 7, pp. 150609–150622, 2019.

[174] J. S. Teh, M. Alawida, and Y. C. Sii, "Implementation and practical problems of chaos-based cryptography revisited," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102421.

[175] M. Alawida, J. S. Teh, A. Samsudin, and W. H. Alshoura, "An image encryption scheme based on hybridizing digital chaos and finite state machine," *Signal Process.*, vol. 164, pp. 249–266, Nov. 2019.

[176] W. H. Alshoura, Z. Zainol, J. S. Teh, and M. Alawida, "A new chaotic image watermarking scheme based on SVD and IWT," *IEEE Access*, vol. 8, pp. 43391–43406, 2020.

WAFA' HAMDAN ALSHOURA received the B.Sc and M.Sc. degrees in computer science from the Al-Zaytoonah University of Jordan, Jordan, in 2012 and 2017, respectively. She is currently pursuing the Ph.D. degree with the School of Computer Sciences, Universiti Sains Malaysia. Her research interests include digital watermarking and hash function.

ZURINAHNI ZAINOL received the bachelor's degree in computer sciences from Universiti Kebangsaan Malaysia (UKM)/Universiti Teknologi Mara (UITM), the master's degree in artificial intelligence from Universiti Sains Malaysia (USM), and the Ph.D. degree in computer science from the University of Hull, U.K., in 2012. She is currently an Associate Professor with the School of Computer Sciences, Universiti Sains Malaysia, where she also holds the deputy dean position for academic, career, and international. She has published papers in international journal, conferences, and book chapters. Her research interests include data modeling, XML database schema, optimization algorithm, and information retrieval in multidisciplinary domain, such as medical, health, biological, and education data.

JE SEN TEH received the B.Eng. degree (Hons.) majoring in electronics from Multimedia University, Malaysia, in 2011, the M.Sc. degree in computer science from Universiti Sains Malaysia, in 2013, and the Ph.D. degree from the School of Computer Sciences, Universiti Sains Malaysia, in 2017. He is currently working as a Senior Lecturer with Universiti Sains Malaysia. His research interests include cryptography, cryptanalysis, random number generation, machine learning, and chaos theory.

MOATSUM ALAWIDA received the Ph.D. degree in computer science/cybersecurity (cryptography) from the School of Computer Sciences, Universiti Sains Malaysia, in 2020. He published more than 15 articles in high impact factor journals. His research interests include chaotic systems, chaos-based applications, multimedia security, blockchain, cybersecurity, Quantum-based cryptography, and cryptography. He has also served as a referee for some renowned journals, such as IEEE TRANSACTIONS ON CYBERNETICS, *Signal Processing*, *Information Sciences*, *Journal of Information Security and Applications*, IEEE ACCESS, *Wireless Personal Communications*, the *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, *Optik*, *Optics & Laser Technology*, *IET Information Security*, *IET Image Processing*, *Security and Communication Networks*, *Chaos, Solitons & Fractals*, *Physica A: Statistical Mechanics and its Applications*, and *Signal Processing: Image Communication*.

ABDULATIF ALABDULATIF (Member, IEEE) received the M.Sc. and Ph.D. degrees in computer science from RMIT University, Australia. He is currently an Assistant Professor with the College of Computer, Qassim University, Saudi Arabia. His research interests include applied cryptography, cloud computing, and data mining.