A Survey of Digital Watermarking Techniques for Data Protection in Cloud Computing

Abbas Nna Halima
Department of Computer Science
Federal University of Technology
Minna, Nigeria
Halimanna1983@gmail.com

Mohammed Danlami Abdulmalik
Department of Computer Science
Federal University of Technology
Minna, Nigeria
drmalik@futminna.edu.ng

Solomon Adelowo Adepoju
Department of Computer Science
Federal University of Technology
Minna, Nigeria
solo.adepoju@futminna.edu.ng

Enesi Femi Aminu
Department of Computer Science
Federal University of Technology
Minna, Nigeria
enesifa@futminna.edu.ng

2022 5th Information Technology for Education and Development (ITED) | 978-1-6654-9370-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/ITED56637.2022.10051180

Abstract **- Recently digital watermarking techniques played an essential role in protecting and authenticating the copyright of multimedia content in a cloud. Based on the literature, there are several digital watermarking techniques used for data protection in cloud computing. However, each of these techniques has its own limitations such as high levels of piracy, theft, and unauthorized distribution of multimedia content. This Survey employs a content-based analysis approach to investigate the watermarking techniques that are more secure, imperceptible, and robust against various kinds of multimedia attacks. The survey shows that the hybridization of watermarking techniques and feature descriptors is more efficient in comparison to a single watermarking technique. This research work concludes that the hybridization technique and use of descriptors are more secure.**

Index Terms: Digital Watermarking, multimedia contents, feature descriptors, authentication, robustness, hybridization.

I. INTRODUCTION

Cloud computing has emerged as one of the most efficient computing paradigms in the world of information technology in recent years. This is due to an increase in parallel, grid-distributed, and other paradigms form of computing [1]. In Cloud, computing customers are offered three basic service models; the SaaS model, the IaaS model, and the PaaS model. The SaaS model which means Software as a service is primarily designed for the end user who has to use the software in performing their day-to-day activities. However, the Platform as a service (PaaS) is primarily designed for developers that require a platform environment to develop their software and application [1]. While Infrastructure as a service (IaaS) is built for network architect development requirement service. User data and information can be stored and accessed via the cloud without the knowledge of data located in the cloud. Security in cloud computing has been frequently raised as one of the most pressing issues in computing. In other to establish ownership authenticity and prevent the issues of data misusing, multimedia information or content can be secure using the watermarking approach. Cloud computing has three categories which include public cloud computing; this cloud computing service are been provided by a third-party body that is built on the internet, this service is accessibly by any customer or users who want to use it by paying for the specific service they are consuming [2]. Secondly, Private Cloud computing services are being provided or accessed via the internet or a private network. In this category, services are offered to only a specific set of users, though a high level of security and privacy is implemented through internet hosting and firewall. Finally, the hybrid cloud service provides a combination of private and public cloud services to users. Within the hybrid cloud, both public and private clouds can be managed independently but applications and data can be distributed or shared among the clouds in the hybridized cloud (private and public cloud) [2].

The massive inventions of digital multimedia products lead to the high demands on authenticity, protection, and security of any digital multimedia content [3]. The potential solution is presented with the inventions of digital watermarking approaches, which tends to secure ownership rights and interest by embedding certain form of information secretly that is only known to the owner into the digital media intended to be secure.

Furthermore, watermarking can be defined as the method of embedding a dual or single watermark item into digital multimedia content such as audio, images, and video content [3]. The three types of watermarking techniques are spatial domain, frequency domain, and hybrid domain. The most common examples of frequency domain watermarking techniques or approaches include SVD (Singular Value Decomposition) and the Karhunen-Loeve Transform (KLT). The spatial domain approaches are basically the initial techniques adopted, in which embedding of the watermarked image can be achieved by modifying the pixels of the image directly [3]. The spatial domain is widely used due to the advantages derived in terms of low computational cost and accessibility to implementation. For example, the LSB (Least Significant Bit), spectrum, and correlation base are the most common spatial domain algorithm. Additionally, there are three types of watermarking systems; blind watermarking, non-blind watermarking, and semi-blind watermarking. Although the original image is not required in the blind watermarking, because the techniques only extract the watermarked image. The blind watermarking approach is

978-1-6654-9370-3/22/$31.00 ©2022 IEEE

widely adopted in the field of healthcare and copyright protection. The Nonblind approach of watermarking copies the source or original image and the watermark that is embedded alongside the test data for extraction, the methods are frequently used in covert communication and copyright protection. The Final method of watermarking system is the Semi blind watermarking, this deprived to requiring the original data for detection. In the area of image authentication and CAD models, semi-blind watermarking is adopted [4].

Digital Content or media can also be secured using Cryptography techniques. After the media content has been decrypted, there will be no further protection on the media content, hence this results in illegal access to private information. This limitation is being rectified using digital watermarking. This has improved multimedia content protection and authentication without reducing the visual quality of the original image. A certain factor is considered while securing multimedia content, this includes the robustness of the image, the ability to authenticate and validate ownership, security, capacity, and imperceptibility. All these factors determine the efficiency of various watermarking algorithms [5]. However, the features descriptors algorithm has a significant positive impact on almost all computer vision, this area includes object tracking, mobile robot mapping, panorama stitching, and 3D surface reconstruction by taking the description and detection of several points on an image. Example of feature detection algorithms includes the SURF algorithm, SIFT algorithm, ORB algorithm, and finally the BRIEF algorithm [6]. Features descriptors are divided into two main classes namely, floating point descriptors and binary descriptors. The most common example of floating-point descriptor is SIFT and SURF while BRIEF, ORG, BRISK, and FREAK are a typical example of binary descriptors. Feature descriptions are known to be at the core of various computer vision technologies, such as the reconstruction of 3D images, object recognition, image retrieval, and localization of the camera. Technologies that can handle a large amount of data, and run-on modern devices with minimum computational power are in high demand in the field of information technology [6]. Hence, the development of these fast descriptors algorithms is growing exponentially with the capability of fast computational description, fast feature matching, efficient memory utilization, and accurate feature description [7]. Various feature descriptors algorithm has been developed. These include Scale Invariant feature transform (SIFT) which is now described as the cutting edge to feature descriptors due to its robustness against rotation and scaling attacks. In addition to the SIFT algorithm, other faster descriptors are developed that include Speed Up Robust Features (SURF), and Binary Robust Independent Elementary Features (BRIEF) [8]. The brief algorithm is incredibly good in performance and yet still a simple feature descriptor. Other descriptors include; Features from accelerated segment tests (FAST) and rotated binary robust independent elementary features (ORB). [9], [10].

The research problem identifies that security has been a challenging aspect for the past decade. The Cybertheft of multimedia content has increased exponentially due to the advancement in technology. [11] already stated that multimedia content should include authenticity and ownership stamps due to the theft, piracy, or modification of this multimedia. Many techniques have been proposed to secure multimedia data (images or video). A comprehensive survey on existing and trending (either single or hybrid) techniques has not been diligently analyzed or surveyed.

Consequently, this research work aims to review previous research papers that adopt single techniques and hybrid watermarking techniques. In addition, feature descriptors techniques can drastically improve watermarking techniques in terms of capacity, speed, robustness, imperceptibility, and security.

The goal of this study is to undertake a comprehensive review of watermarking schemes for safeguarding multimedia content. The considered domain in this survey includes a frequency domain, a spatial domain, a hybrid domain, and feature descriptors along with their hybridization.

In this survey, the contribution achieved is that the hybridization of watermarking techniques and the use of feature descriptors are found more effective, based on the majority of reviewed papers that identify hybridization techniques and descriptors in terms of merits (strength).

II. LITERATURE REVIEW

A. Survey Approaches

Many approaches have been proposed to improve digital watermarking, in protecting multimedia content from piracy. A comparative analysis will be employed based on existing single or large algorithms (methodology), merits (the advantages of using these algorithms), and demerits (the limitation or drawbacks) in terms of robustness, imperceptibility, security, and capacity [12].

B. Approaches of Digital Watermarking Algorithm

Digital information has been protected using various watermarking schemes over the years. This technique helps in verifying the integrity and authenticity of the carrier signal. Technically watermark could be a text or secondary image that is embedded into another host image for protection [13]. Digital watermarking is being widely used in areas such as copyright protection, broadcast monitoring, tamper detection, image processing, authenticity verification, and the like.

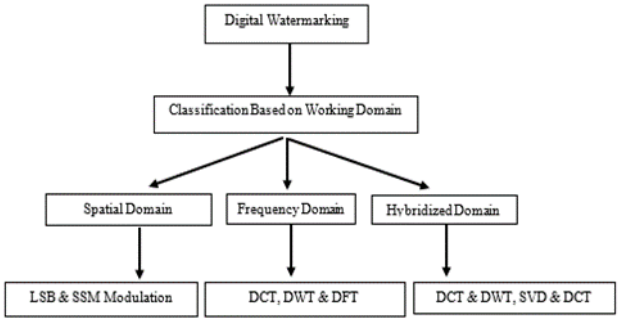

Fig.1: Pictorial depiction of various categories of digital watermarking

i. Spatial Domain Techniques:- Techniques under the spatial domain branch work quite well on image pixels, by modifying the pixel value for embedding watermark data. The Least Significant Bit (LSB) is rank the most frequently adopted techniques use under the spatial domain. The primary or main benefit of spatial domain watermarking algorithms is the simplicity, low computational complexity, and less time consumption. the estimated computational speed of spatial domain techniques is very fast in comparison to the frequency domain and it can be easily applied to any image. One potential drawback of spatial domain techniques is the less robustness to many attacks than that of the frequency domain techniques [3], [13]

ii. Frequency Domain Techniques:- The frequency domain is more efficient than the spatial techniques. Images are represented in form of frequency. Hence, the frequency domain techniques are more adopted in digital watermarking in comparison to the spatial domain techniques. The major aim of this technique is to take a host image and embed a watermark in the spectral coefficients. The most frequently used algorithm in the frequency domain includes the Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), Singular Value Decomposition (SVD), and finally the Discrete Cosine Transform (DCT) [13]

Spatial Domain and hybridize watermarking algorithms

The mode widely used digital watermarking method in the spatial domain is described in this section.

1. Least Significant Bit (LSB): - Considering the spatial domain the least significant bit approach for watermarking is the simplest, and it holds a small amount of relevant information. Hence, LSB modification on the image does not cause visible changes. Watermark embedding is easier using LSB by randomly selecting pixels of the source image. For a given image each pixel is represented using an 8-bit stream and the watermark is added to selected pixels of the host image. Considering the implementation point of view LSB approach is easier [14]. In addition, the LSB does not result in severe distortion of the image. It is however not highly resistant to attacks [13].

2. Spread Spectrum Modulation Techniques: - The spectral-based modulation techniques generate energy at different discrete frequencies. Increase in resistance to natural interference as to be established for communication to be established. The SSM watermarking algorithm embeds information and data in the context of image watermarking. Hence, when the context of image watermarking is applied it embeds information or messages by adding up the cover image with a little pseudo-noise signal modulation [13].

Frequency Domain and hybridize watermarking algorithm

1. Singular Value Decomposition (SVD)

SVD is an effective technique for handling matrix problems generally. SVD decomposes a rectangular matrix into two orthogonal matrices and a single diagonal matric [15]. Singular value decomposition is a very sophisticated numerical analysis approach for metrics that produce the smallest truncation error [16]. It's a widely used metric because of the total possible level of freedom offered by the matrices, which is equal to the input cover image. The key property of SVD in image processing is the singular value of an image that has good stability, the intrinsic algebraic image properties are represented using singular value [17].

2. Discrete Cosine Transform (DCT)

The discrete cosine transform is used to convert spatial domain signals into frequency domain signals, hence it is used in signal processing. Various fields such as pattern recognition, data compression, and other aspects of image processing. However, the discrete cosine transform is more robust than that of the spatial domain watermarking algorithm. The DCT algorithm is similar to the discrete Fourier Transform; though, it represents data in a form of frequency space not in amplitude space. In DCT signals are converted into elementary frequency components [13].

3. Discrete Wavelet Transformation (DWT)

Many signal processing applications adopt the use of discrete wavelet transformation. Applications such as video, audio compression, and wireless antenna distribution, are used in removing noise from audio. The signal of DWT changes in relation to time, which makes it suitable for most applications. The wavelets' energy is centrally based on time and this makes it more suitable for transient analysis, and varying time signals. The discrete wavelet transformation is faced with the tradeoff between robustness and imperceptibility [13]. In DWT multi-resolution representations of the image are given in a simple framework to describe image information. Analysis of the signal is carried out in different resolutions by the DWT. Images are decomposed into high-low and low-frequency quadrants

4. Discrete Fourier Transform (DFT)

Discrete Fourier transform is well known due to its high robustness to attacks such as cropping, rotation, translation, and scaling attacks. Images are spat into sine and cosine forms in DFT. They are two main classifications of DFT techniques based on the approach of embedding which includes; direct embedding (though, DFT magnitude and the phase coefficient are adjusted for watermark embedding) and template base embedding (which proposed the use of template). Templates are basically the structure that is embedded in the DFT domain and is used for computing the transformation factors when the image goes under transformation. The

central component which contains the low frequency is the primary component of DFT [13].

5. Hybridized DWT and SVD Banjarnahor et al [18] Techniques

Discrete wavelet Transformation and Singular Value Decomposition hybridization are adopted in various research papers such as the work of Singh et al [13], Banjarnahor et al [18], Yadav et al [19], and many others. This study considers hybridized SVD and DWT techniques to strive to achieve great security and efficiency in comparison to other frequency domain watermarking. However, the performance of the hybridized techniques is evaluated using the PSNR, SSIM, and NC. Based on this approach the strength of DWT and SVD are merged together. Nonstationary signal processing and image decomposition are carried out using DWT, while the singular value decomposition is utilized in the manipulation of data with minimum loss and data de-noising. The SVD also contributes intrinsic geometric attribute of the image. In this paper, both algorithms are proposed to improve efficiency in terms of robustness and imperceptibility [18]. The techniques show better performance by giving a result of PSNR above 37dB.

6. Hybridized DCT and SVD (Kanhe & Gnanasekaran [20] Techniques.

Few types of research such as Kanhe & Gnanasekaran [21] adopted the hybridization of discrete cosine transform and singular value decomposition, in other to attain a high level of robustness and imperceptibility. this survey work will only consider the research paper of [21], which uses both DCT and SVD transform techniques to achieve a robust image in audio watermarking. This is achieved by selecting the audio signal low-frequency component for embedding the watermark image data, this makes the watermarked audio to be highly robust and imperceptible. The researcher evaluates or measures the robustness of the proposed hybrid techniques using the bit error rate and computed average information loss. The robustness is highlighted using Shannon's entropy to compute the information loss in retrieving the watermarked image. A high value of SNR is confirmed which shows that the hybridized approach is highly imperceptible. high embedding capacity of 6kbps is achieved [16, 17].

7. Hybridized BPNN and DWT Ananth, et al [22] techniques.

Multiple watermarking for images is achieved in this research work of Ananth, et al., [22] which adopts a hybridized Back Propagation Neural Network (BPNN) and Discrete Wavelet Transformation. Using the improved BPNN, watermark images are inserted into multiple cover images, which maximize or improved learning space, and minimum error, and qualified neural networks are extricated with various watermarks as of the embedded images. With this technique. There is an excellent achievement in the visual effect of the watermark schedule and high robustness while extracting the multiple watermarks [22]

8. Hybridized Speed-up robust features (SURF), DCT, and SVD

In the proposed hybridized algorithm, a chaotic is used for watermarking medical images and providing adequate security on medical images. The SVD algorithm is used to decompose or split the original matrix into three different matrices. The watermarked image is produced by merging the watermark image with the cover image using the SURF-DCT-SVD technique. The researchers carried out various research on the proposed method and based on the experimental result it was shown that SVD can enhance the resistance of DCT and SURF-based watermarking schemes to attacks. The proposed watermarking scheme is able to resist JPEG compressional attacks, signal processing, noise addition, and geometric attacks [23].

9. Hybridized watermarking Scheme using SIFT with Reversible Rotation Huang et al [23]

This research work proposed a watermarking method using scale invariant feature transformation (SIFT) to save guide medical data using integer rotation in protecting the confidentiality of medical data. Hence, the position of the original data is extracted using SIFT, the reversible integer rotation algorithm is used to rotate the host image. Steganography data is generated by estimating the distortion and the histogram scale. The variant of the histogram scale is used to embed after applying integer rotation using the angles as the alternative parameter. The method resulted in imperceptible with an average peak signal-to-noise ratio (PSNR) of 50.595 and an average entropy of 5.16 [23].

10. Hybridized RDWT-SVD approach Sharma et al [24]

These watermarking techniques are used for adaptive color image watermarking. Various existing scheme of watermarking uses a grayscale or binary image for watermarking, but the researcher proposed new adaptive and robust techniques for watermarking, the watermark and the host image are both colored images and image with equal dimensionality. Moreover, this technique is improved by scrambling both the colored cover image and watermark image using the map of Arnold chaotic. The redundant discrete wavelet transforms (RDWT) decompose the host image in a smaller matrix of four with equal dimensions, each sub-matrix undergoes a singular value decomposition in other to get the principal component (PC). This approach overcomes the primary security challenge of false error (FPE), which mostly surface in the traditional watermarking scheme using SVD [24]

11. Medical Image Watermarking Based on SIFT-DCT Perceptual Hashing (Lui et al [25]

This approach was developed to solve the issue of medical data protection. The algorithm hybridizes the Scale Invariant Feature Transform and the discrete cosine transform using perceptual hashing. Initially, the approach uses SIFT-DCT perceptual hashing to get the attribute of the main or original medical images, then

quantize it to generate the hashing sequence.in other to encrypt the watermarking and integrate it into the medical image, the hybridizing process uses a chaotic map. Finally, the correlation coefficient of the extracted watermarking and embedding sequence is calculated to show the algorithm's robustness. However, the proposed hybridized algorithm shows the result of good robustness with respect to geometric attacks, conventional attacks, and most important terms of rotation, translation, and cropping [25].

12. A SIFT Feature-based blind watermarking for DIBR

The approach is used for blind watermarking a Depth Image Based Rendering (DIBR). It is a promising method for deducing viewpoint using a monoscopic middle image which is grouped per-pixel depth map. Based on various merit which includes low-cost bandwidth, adjustment of depth condition, two dimensional to three-dimensional compatibility. These advantages make depth image-based rendering gain much attention in the three-dimensional research community. Based on the case of the broadcasting system using DIBR, a malicious adversary can unauthoritatively distribute both a middle view and synthesized virtual view as two-dimension and three-dimension content. However, to protect the copyright of a depth image-based rendering, the Scale Invariant Feature Transform (the SIFT algorithm) feature based for blind watermarking is proposed in this paperwork. The proposed techniques show a low Bit Error Rate for signal processing attacks and geometric distortion processes based on translation and cropping [26].

13. Hybridized DWT, DCT, and SIFT Hamidi et al., [20] technique

The researcher adopts hybridized techniques for copyright protection. The method includes DCT, DWT, and SIFT. However, the major focus of the researchers is to develop a feature-based image watermarking technique, which is capable of withstanding both image processing and geometric modification, while maintaining imperceptibility. The SIFT feature point is registered to be used in the extraction procedure in order to correct the geometric attack, and the DCT and DWT are for embedding. While maintaining imperceptibility, the techniques have proven strength or robustness against traditional image processing attacks and geometric modification [20].

14. Hybridized LBP and DWT Based Fragile watermarking scheme for Image Authentication

The researchers considered merging two techniques for image authentication and fragile-based watermarking. The Discrete Wavelet Transform (DWT) uses better multi-resolution decomposition attribute and the frequency component is low, which contain primary or basic data of an image. Then the low-frequency wavelet coefficients pattern of a local binary pattern is utilized as a watermark feature. Which is now included in the least significant bit. However, this researcher proposes the application of a logistic map to secure the watermark in other to ensure the security of the hybridized logic. The result of this technique presents a higher visual quality. In comparison to other techniques, it has a low watermark payload and also achieved better performance in localization and tamper identification for various attacks [23, 24].

III. FINDINGS

This review gathers and identifies facts and showcases the performance of the most popularly used watermarking approach and hybridize watermarking techniques. Hence, the table below summarizes various approaches adopted in watermarking and feature descriptors domain.

Table 1. Strengths (Merits) and Weakness (Demerits) of the Existing Techniques Reviewed

S/No.	Approach	Usability	Merits	Demerits
A	Least Significant Bit: (LSB)	It converts the host image into a shaded grayscale image, it hides text represented using 8 bits by referencing the converted image.	The LSB is very simple and easy from it point of implementation	This approach is defenseless against the Stegano-analysis. The techniques are not robust to all attack
B	Discrete Cosine Transform (DCT)	The algorithm m is used to carry out signal processing by converting or transforming spatial domain signals into frequency domain signals. It also represents the signal in frequency space rather than using amplitude space	Robust on an image with low pass filtering, contrast brightness, and blurring effect	Not Robust to all geometric attacks such as rotation, cropping, and scaling.
C	Discrete Wavelet Transformation (DWT) algorithm	Widely used in signal preprocessing, such as audio and video compression, noise removal, and simulation of wireless antenna distribution	Scalable in nature and is good in multi-resolution techniques and spatial domain localization.	High computational cost, and it takes a longer time in performing computation.
D	Discrete Fourier Transform (DFT) algorithm	DFT is applied in the area direct embedding or template embedding is required.	The main benefit it is found to be rotation, scaling, and transition (RST) invariant over DCT, DWT and RST. Easily overcome geometric distortion.	Computational inefficient, complex values and more frequency rate are required.
E	Singular Value Decomposition (SVD) algorithm	It is used in image compression, watermarking, de-noising forensics, and analyzing rectangular matrices.	Achieves high stability against variation in histogram equalization, filtering, noise histogram, and compression due to the addition of a weighted watermark.	The major issue of SVD occurs when its use for non-blind watermarking, though not robust to intentional attack in terms of fast extraction from watermark image.
F	Hybridize DWT, SVD Banjarnahor et *al* [18] algorithm	Hybridized techniques are used to secure digital medical images.	It provides higher security and efficiency in comparison to other frequency domains. It also overcomes the limitation of conventional SVD techniques.	Not design for colored images and for videos
G	Hybridize DCT, SVD (Kanhe & Gnanasekaran, [21] Techniques.	The hybridized approach is used to design a more robust image in audio watermarking.	High data payload, low pass filtering, and high pass filtering attack.	It is not Robust to withstand pitch-shifting attacks, random cropping attacks, and time-scale modification attacks.
H	Hybridize BPNN, DWT Ananth, [22] Techniques.	The hybridized techniques are used for multiple watermarking of images	Enable multiple embedding with the advancement of learning space and error reduction. Imperceptibility on watermarking and high robustness on the extracted watermark.	Computationally complex, and computationally inefficient.
I	Hybridize DWT, DCT, and SIFT Hamidi et al., [20] Techniques.	The primary usage of this approach is to protect the owner's copyright.	High robustness against image processing and geometric manipulation attack while high imperceptibility is maintained	No usage of a meta-heuristic algorithm in finding optimal watermarking strength.
J	Hybridize SIFT, DCT Liu, et al., [25] Perceptual Hashing Techniques.	The hybridized approach is used to secure medical data and images.	Highly robust to translation, rotation, and shared attack. It is also applicable in the field of identification	Not robust to other attacks such as time scale attacks, shifting attacks, image processing attacks, and the like.
K	Hybridization of SURF and DCT Utami *et al.,* [23]on SVD Techniques.	Robust hybridization for watermarking and securing medical images.	The hybridize robust scheme is able to resist JPEG compressional attack, signal processing, noise addition, and geometric attack	Not robust to other image's extensional attack apart from JPEG compression attack.

L	Hybridization of LBP and DWT Wang et al., [26] techniques based on Fragile watermarking.	Fragile watermarking hybridize approach for image authentication.	Higher image quality, resist various attacks and locate tempered areas accurately with minimum payloads.	The hybridized technique is not capable of detecting edge region that is tempered.
M	Novel LBP Wang et al., [9] techniques for blind feature image steganography	The techniques are used in preserving the local structure of the cover image in the resulting steganography image.	High embedding capacity and robustness in stegno-analysis comparison to LSB	The techniques are unable to handle payload specific for hand-crafted descriptors use in embedding data.

IV. RECOMMENDATION

In this study, thirteen (13) different hybridized techniques have been elaborately analyzed accordingly. Six techniques from the watermarking scheme are looked into, five hybridization techniques from both watermarking domain and feature descriptor have been surveyed, from the spatial domain two algorithms are showcased, and finally, eleven watermarking techniques from the frequency domain are comprehensively explained. It is observed in this work that the hybridization of watermarking techniques and feature descriptors has improved the robustness, capacity, security, and imperceptibility of multimedia content. based on the efficient digital description and matching capability of feature descriptors on multimedia content, even in a situation where the multimedia content is distorted. Considering table 1, The research approach that utilizes both domain techniques (watermarking and feature descriptors) help to build a better and more robust system in term of rotation attack, translation attack, scale attack, and shared attack, and it is not limited to other geometric attacks and compression attack. However, a single watermarking technique is not as robust, imperceptible, and secure as paperwork with hybridized techniques. It is recommended to adopt a hybrid approach to support each technique's strengths and limitations in a merging technique. Furthermore, if needs warrant to enhance digital content security, feature descriptor has shown great promising strength.

V. CONCLUSION AND FURTHER STUDIES

In this paper, twenty-six (26) existing research papers on both single and hybrid approaches in watermarking techniques and feature descriptors have been surveyed. This includes their usability or functionality, with corresponding advantages (merits) and limitations (demerits). The capability of each technique in terms of robustness, imperceptibility, and capacity is also comprehensively stated in table 1. It identifies that hybridize techniques are more robust, imperceptible, and secure than adopting single techniques. However, the adoption of feature descriptors in recent work has shown better results in terms of robustness and capacity of multimedia content while still maintaining its quality, feature descriptors are currently the core of many multimedia processing technologies.

future studies should consider surveying and comparing machine learning techniques and deep learning approaches to achieve greater levels and much stronger security, robustness, and imperceptibility of multimedia content.

REFERENCES

[1] T. Alam, “Cloud Computing and its role in the Information Technology,” Transactions on Sustainable Digital Innovation, Madinah, vol. 1, no. 2, pp.108–115, https://doi.org/10.34306/itsdi.v1i 2.103, 2020.

[2] P. Srivastava and R. Khan, “A Review Paper on Cloud Computing,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 8, no. 6, p. 17, 2018, doi: 10.23956/ijarcsse.v8i6.711..

[3] N. Agarwal, A. K. Singh, and P. K. Singh, “Survey of robust and imperceptible watermarking,” Springer. Multimed. Tools Appl., vol. 78, no. 7, pp. 8603–8633, doi: 10.1007/s11042-018-7128-5, April 2019.

[4] N. R. Zhou, W. M. X. Hou, R. H. Wen, and W. P. Zou, “Imperceptible digital watermarking scheme in multiple transform domains,” Multimedia Tools and Applications., vol. 77, no. 23, pp. 30251–30267, 2018, doi: 10.1007/s11042-0186128-9..

[5] A. P. Tafti et al., “A comparative study on the application of SIFT, SURF, BRIEF and ORB for 3D surface reconstruction of electron microscopy images,” Computer Methods Biomech. Biomed. Eng. Imaging Vis., vol. 6, no. 1, pp. 17–30, 2018, doi: 10.1080/21681163.2016.1152201

[6] S. Y. Tan, H. Arshad, and A. Abdullah, “Distinctive accuracy measurement of binary descriptors in mobile augmented reality,” PLoS One, Beijing, China, vol. 14, no. 1, pp. 1–18, 2019, doi: 10.1371/journal.pone.0207191.

[7] M. Calonder, V. Lepetit, M. Özuysal, T. Trzcinski, C. Strecha, and P. Fua, “BRIEF: Computing a local binary descriptor very fast,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 34, no. 7, pp. 1281–1298, 2012, doi: 10.1109/TPAMI.2011.222.

[8] J. Zhang, X. Liu, and X. Liu, “Design of Binary Robust Independent Elementary Features through Compressive Sensing View,” Int. J. Appl. Phys. Math., vol. 5, no. 1, pp. 67–75, 2015, doi: 10.17706/ijapm.2015.5.1.67-75.

[9] T. Wang, Z. Wang, Y. Cao, Y. Wang, and S. Hu, “A multi-BRIEF-descriptor stereo matching algorithm for binocular visual sensing of fillet welds with indistinct features,” Journal of Manuf. Process., vol. 66, no. April, pp. 636–650, 2021, doi: 10.1016/j.jmapro.2021.04.031.

[10] M. Calonder, V. Lepetit, C. Strecha, and P. Fua, “BRIEF: Binary robust independent elementary features,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6314, no. 4, pp. 778–792, 2010, doi: 10.1007/978-3-64215561-1_56.

[11] M. Abdel-Basset, M. Mohamed, and V. Chang, “Neutrosophic Multi-Criteria Decision Analysis (NMCDA): A framework for evaluating cloud computing services,” Elsevier, Futur. Gener. Comput. Syst., vol. 86, pp. 12–29, 2018, doi: 10.1016/j.future.2018.03.014.

[12] O. P. Singh, A. K. Singh, G. Srivastava, and N. Kumar, “Image Watermarking Using Soft Computing Techniques: A comprehensive survey A comprehensive survey,” Multimedia

Tools and Applications, Springer Nature, vol 80(7), pp. 30367–30398, 2021, doi: 10.1007/s11042-020-09606-x.

[13] R. Rawat, N. Kaushik, and S. Tiwari, "Digital Watermarking Techniques," Int. J. of Advan. Res. in Comp. and Comm Eng, Dehradun, India, vol. 5, no. 4, 2016, doi: 10.17148/IJARCCE.2016.54123.

[14] K. Bansal, A. Agrawal, and N. Bansal, "A survey on steganography using least significant bit (LSB) embedding approach," 4th International Conference on Trends in Electronics and Informatics (ICOEI) (48184), IEEE, 2020, no, pp. 64– 69, doi: 10.1109/ICOEI48184.2020.9142896.

[15] N. Singh, "Suitability of Singular Value Decomposition for Image Watermarking," 2019 6th Int. Conf. Signal Process. Integr. Networks, pp. 983–986, 2019. Corpus ID: 155107336, doi:10.1109/SPIN.2019.8711749

[16] J. Dongarra et al., "The singular value decomposition: Anatomy of optimizing an algorithm for extreme scale,"Manchester Research Explore SIAM Review, vol. 60, no. 4, pp. 808–865, 2018, https://doi.org/10.1137/17M1117732.

[17] D. M. K, "SVD based Image Watermarking Scheme," International Journal of Computer Applications (IJCA) Special Issue on "Evolutionary Computation for Optimization Techniques, 1(4) pp. 21–24, ECOT 2010. doi: 10.5120/1531-134

[18] J. Banjarnahor et al., "Digital Watermarking For Medical Images Using Dwt and Svd Technique," 2021, IOP Conf. Series: Materials Science and Engineering 1084 (2021), doi: 10.1088/1757899X/1084/1/012034.

[19] B. Yadav, A. Kumar, and Y. Kumar, "A Robust Digital Image Watermarking Algorithm Using DWT and SVD" Soft Computing: Theories and Applications. Advances in Intelligent Systems and Computing, vol 583, pp. 25–36. Springer, Singapore. 2018, https://doi.org/10.1007/978-981-10-5687-1_3.

[20] M. Hamidi, M. El Haziti, and H. Cherifi, "A Hybrid Robust Image Watermarking Method Based on DWT-DCT and SIFT for Copyright Protection,", Journal of Imaging 2021, 7(10), 218; 2021, https://doi.org/10.3390/jimaging7100218.

[21] A. Kanhe and A. Gnanasekaran, "Robust imagein-audio watermarking technique based on DCT-SVD transform," Eurasip J. Audio, Speech, Music Process., vol. 2018, no. 1, pp. 1– 12, 2018, doi: z10.1186/s13636-018-0139-3.

[22] C. Ananth, M. Karthikeyan, N. Mohananthini, S. Saravanan, and M. Swathisriranjani, "Multiple watermarking for images using backpropagation neural network and DWT," Int. J. Eng. Adv. Technol., India, vol. 9, no. 1, pp. 4088–4093, 2019, doi: 10.35940/ijeat.A1327.109119.

[23] X. Huang, "A New Watermarking Scheme Based on SIFT Feature Points with Reversible Rotation," 2019 First Int. Conf. Digit. Data Process., pp. 59–64, doi: 10.1109/DDP.2019.00021.

[24] 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. J., vol. 84, p. 105696, 2019, doi: 10.1016/j.asoc.2019.105696.

[25] J. Liu, J. Li, J. Chen, X. Zou, J. Cheng, and J. Liu, ''Medical Image Watermarking Based on SIFT-DCT Perceptual Hashing'' International Conference on Cloud Computing and Security, (ICCCS). vol 11066, pp 334–345, Springer, Cham. 2018, https://doi.org/10.1007/978-3-030-00015-8_29

[26] H. Karajeh and M. Maqableh, "An Imperceptible, Robust, And High Payload Capacity Audio Watermarking Scheme Based on The DCT Transformation and Schur Decomposition," Analog Integr. Circuits Signal Process., vol. 99, no. 3, pp. 571–583, 2019, https://doi.org/10.1007/s10470-018-1332-0