A HYBRID BRIEF-SVD WATERMARKING TECHNIQUES FOR DATA PROTECTION IN CLOUD COMPUTING

BY

ABBAS, Halima Nna
MTech/SICT/2019/10893

DEPARTMENT OF COMPUTER SCIENCE
FEDERAL UNIVERSITY OF TECHNOLOGY
MINNA

JULY, 2023

A HYBRID BRIEF-SVD WATERMARKING TECHNIQUES FOR DATA PROTECTION IN CLOUD COMPUTING

BY

ABBAS, Halima Nna
MTech/SICT/2019/10893

A THESIS SUBMITTED TO THE POSTGRADUATE SCHOOL FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA, NIGERIA IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF TECHNOLOGY (MTech) IN COMPUTER SCIENCE

JULY, 2023

ABSTRACT

In the recent world with developing technologies, information is collected, stored digitally, and transmitted. While transmitting the information digitally, security and authenticity remain the main issue. Watermarking is the technology that ensures the authenticity and security of multimedia images. Digital watermarking techniques played an essential role in protecting and authenticating the copyright of multimedia content. There are several digital watermarking techniques used for image and data protection in cloud computing. However, because of the poor image quality, the watermarking techniques currently in use are inefficient, which presents a security challenge. The crucial requirements for designing an efficient watermarking scheme are robustness, imperceptibility, capacity, and security. To meet all of these requirements simultaneously is nearly impossible. Therefore, this research study developed a hybridized watermarking technique that is Binary Robust Independent Elementary Features (BRIEF) and Singular Value Decomposition (SVD), in order to enhance robustness, imperceptibility, and security. The proposed hybridized scheme was used to perform experiment using image data obtained from Kaggle Repository. The performance of the proposed hybrid technique was subjected to an evaluation using four metrics namely; Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Mean Square Error (MSE), and Means Absolute Error (MAE). Thus, the following results were obtained: PSNR value of 34.29dB, SNR of 11.44dB, MSE 2.8 MAE 6.88 respectively, making it the best performing technique compared to that of the existing techniques which were only based on PSNR with DCT value of 30dB and FRFT, DCT value of 33.518dB. BRIEF-SVD performed efficiently well in terms of PSNR, SNR, MSE, and MAE. This study concludes that the hybridization technique and use of feature descriptors are more robust and secure for image multimedia contents.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

API: Application Programming Interfaces

AWS: Amazon Web Services

BCR: Bit Correlation Error

BER: Bit Error Rate

BRIEF: Binary Robust Independent Elementary Features

BRISK: Binary Robust Invariant Scalable Keypoints

CIA: Confidentiality Integrity and Availability

CPU: Central Processing Unit

DCT: Discrete Cosine Transform

DFT: Discrete Fourier Transform

DWT: Discrete Wavelet Transform

FAST: Features from Accelerated Segment Test

FRFT: Fractional Fourier Transform

GCE: Google Computer Engine

IWT: Integer Wavelet Transform

LSB: Lease Significant Bit

MAE: Means Absolute Error

MSE: Means Square Error

NC: National Correlation

NIST: National Institute of Standard and Technology

PC: Personal Computer

PSNR: Peak Signal to Noise Ratio

PWA: Patch Work Algorithm

QIM: Quantization Index Modulation

RGB: Red Green Blue Images

SIFT: Scale Invariant Feature Transform

SNR: Signal to Noise Ratio

SSM: Spread Spectrum Modulation

SURF: Speed up Robust Features

SVD: Singular Value Decomposition

CHAPTER ONE

1.0 INTRODUCTION

1.1 Background to the Study

Multimedia data such as texts, images, audio, and videos, are now transmitted over the internet, mobile devices, and the cloud. Many multimedia data are recreated and circulated by imposters without any copyright during the voyage of these multimedia assets from one location to another via any of the mediums of mobile, internet, and cloud (Thanki *et al*., 2017).

Cloud computing is a methodology for quickly provisioning and releasing a shared pool of configurable computing resources such as networks, storage, servers, services, and applications (Khajanchi, 2019) with minimal administration effort and service provider involvement (Anitha & Patil, 2016). Similarly, Sujan & Devi, (2015) define cloud computing as a computing paradigm for managing and delivering services over the internet, it is also an integrated concept of parallel and distributed computing that shares resources like hardware, software, and information to computers or other devices on demand. Cloud computing has recently become one of the most popular computing paradigms in the field of information technology, with many organizations shifting to the cloud for data storage rather than using a local storage system (Anitha & Patil, 2016).
The current computing paradigms in cloud computing include parallel computing, grid computing, and distributed computing. There are three major deployment models of cloud computing, these are public cloud, private cloud, and hybrid cloud (Alam, 2020).

The literature of (Anitha & Patil, 2016; Sujan & Devi, 2015) by their definitions clearly shows that cloud computing plays an important role in the lifestyle of humans in the IT world of today. Therefore, the nonexistence of cloud computing in our world today would

vehemently make life difficult for everyone because the storage and protection of data are extremely important and significant in the field of information systems.

Cloud computing looks like a big black box, what it contains is usually not visible to the clients, this means the clients do not know what happens inside the cloud, however, its rapid advancement has gained so much popularity across the World Wide Web (Anitha & Patil, 2016). According to Sarwar *et al*., (2017), cloud computing is quickly accessible to data, files, programs, and services from a web browser over the internet, the researcher claimed that cloud computing stores software programs and other computing applications in a central location.

Abdel-Basset *et al*., (2018) their work presented that cloud computing permits consumers and businesses to use the application without installation and access their personal files on any computer with internet access. Furthermore, users can also store their own data, storage, and application on the cloud. Cloud computing allows sharing of a single application or physical resources among multiple clients, while load balancing can be handled by virtualization (Rashid & Chaturvedi, 2019).

A comprehensive purview of cloud computing cannot be overemphasized; however, there are major areas in which its application has made life easy for humanity such as cloud computing for mobile health applications, cloud computing in academic institutions, cloud computing in library automation and cloud computing in E-learning, all of these benefits according to (Sarwar *et al.*, 2017) are possible and easily accessible due to the fact that cloud computing is a model that provides high-performance computational service at a minimal cost. The most common and more familiar application of cloud computing is the automatic software update which happens even on mobile devices (Ahmad, 2018), other benefits may include, lower IT infrastructure and computer costs

for users, fewer maintenance issues, instant software updates, backup, and recovery, cost saving, flexibility, better mobility, improved performance, performance and scalability, improved communication and most of all, increased storage space (Khajanchi, 2019).

Despite all the opportunities of cloud computing, it is prone to some setbacks among which data security is the biggest challenge (Lee *et al.*, 2018). Data security is one of the biggest concerns in cloud computing. The data to be sent should only be accessible by authorized users, numerous different techniques are introduced by computing researchers for data protection (Sarwar *et al*., 2017). According to Malik & Kumar, (2016) the growing use of the internet has made access to data easier and this has increased the tempering of data which has led to the problems of data insecurity, which needs to be considered in today's technological world for the transmission of data from one place to another. Therefore, the increasing rate of data hacking, which has made access to private data simpler, has prompted users to secure their data using better techniques and algorithms. One of the best approaches to overcome this challenge is the use of a digital watermarking technique.

Digital watermarking is a security technology that embeds signals and secret information called watermarked within digital media content such as images, audio, and video. (Souley & Adamu, 2017). It ensures security privacy and ownership authentication of the media content being watermarked.

Thaiyalnayaki and Devi, (2018), define digital watermarking as a group of bits inserted into a digital data (audio or video, or image) file that identifies the files copyright information. Usually watermarking has been used in currency notes, government documents, passports for security features, and stamp papers for legal purposes, watermarking is very beneficial for identifying the document of any authorized person.

The sole aim of watermarking is securing the identity of our data and multimedia; however, the integrity of these securities is always faced with outside attacks. Such attacks on watermarking can be classified into five major types of watermarking attacks, which are Geometry attack, Removal attack, Protocol attack, copy attack, and Cryptography attack (Wadhera *et al.*, 2022).

According to (Malik & Kumar, 2016) Techniques such as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Frequency Domain Technique (FDT), Discrete Wavelet Transform (DWT), and Integer Wavelet Transform (IWT) are the major forms of techniques used in securing data in cloud computing. However, the techniques are not fully robust against one or the other attacks because DWT does not consider the security of the watermarking image, a wide range of rotational attacks are very possible, FDT protection technique is not against all possible attacks, DCT does not ensure better imperceptibility and is not robust against noise, filtering, JPEG compression, and geometric attacks, DFT has a drawback of truncating the coefficient of the signal and there is loss of information (Joshi *et al.*,2017). The intended proposed techniques to overcome the robustness, capacity, imperceptibility, and security challenges faced by data in cloud computing are the combination of Singular Value Decomposition (SVD) and Binary Robust Independent Elementary Features (BRIEF). In the SVD technique, the information of the watermarking is added to the singular matrix which does not affect image quality and also takes care of the robustness and the imperceptibility of the image, SVD have a high security and efficiency as compared with other watermarking techniques, techniques such as DWT, DCT, IWT and DFT (Savaridass *et al.*, 2021). Similarly, SVD for watermarking ensures robustness against most image processing operations such as image filtering, image compression, image hiding, and noise reduction (Singh *et al.*, 2019). BRIEF is rotation invariant and translation invariant which makes it

ideal to withstand various kinds of image processing attacks (Tan *et al.,* 2019). However, BRIEF descriptor was designed as a result of the increased use of mobile devices with higher resolution images, BRIEF uses XOR operation (Bit wise operation) to calculate Hamming distance during feature matching which can be computed efficiently and extremely fast on modern CPUs. BRIEF descriptor easily outperforms other feature point descriptors such as SIFT, SURF, BRISK, FAST, and K-KAZE in terms of speed and recognition rate (Wang *et al.,* 2021). BRIEF is a binary descriptor that is simple, efficient, and fast to compute, this descriptor has achieved the best performance and accuracy in pattern recognition and uses Gaussian smoothening or (Kernel Smoothening) to smoothens the images and enhance its robustness (Kortli *et al*., 2020).

1.2 Statement of the Research Problem

The application of several watermarking techniques such as Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Integer Wavelet Transform (IWT) has been hybridized in some literature. This is to achieve a certain degree of robustness, security, capacity, and imperceptibility under different types of attacks. However, the watermarking techniques used are deficient because of poor image quality (Mohammed *et al.,* 2021); consequently, it throws up the challenge of insecurity. The essential requirements for designing an efficient watermarking system are robustness, imperceptibility, capacity, and security. However, meeting all of these requirements concurrently is nearly impossible. Begum & Uddin, (2020) faced with the computational complexity of watermarking embedding and extraction. The existing singular digital image watermarking techniques cannot obtain all the desire goals, such as imperceptibility, robustness, security, and capacity simultaneously with perfection. Therefore, this research proposes a hybrid watermarking scheme that would combine Binary Robust Independent Elementary Features (BRIEF)

and Singular Value Decomposition (SVD) to address the deficiency of the aforementioned techniques.

1.3 Aim and Objectives of the Study

This research work aims to develop a hybrid watermarking scheme for data protection in cloud computing using hybrid Binary Robust Independent Elementary Features and Singular Value Decomposition techniques. The objectives of this study are to:

i. Hybridize Binary Robust Independent Elementary Features (BRIEF) and Singular Value Decomposition (SVD) to enhance the robustness, imperceptibility, and security of image watermarking techniques
ii. Develop a robust conceptual framework of the watermarking scheme based on the hybridized techniques in objective (i).
iii. Evaluate the performance of the hybridized techniques against the existing technique using Peak Signal Noise Ratio (PSNR), Mean Square Error (MSE), Signal Noise Ratio (SNR), and Means Absolute Error (MAE) performance metrics.

1.4 Scope and Limitation of the Study

In recent years, several research works have been proposed in the field of watermarking. However, there are still various limitations and challenges in the development of watermarking techniques. In this proposed research work, the scope will be mainly focused on multimedia images by developing a watermarking scheme for data protection in cloud computing using a hybridized technique considering Singular Value Decomposition (SVD) and Binary Robust Independent Elementary Futures (BRIEF) techniques in watermarking. Conversely, in this proposed research work, other types of multimedia such as textual and video are not considered.

1.5 Significant of the Study

The significance of this study are as follows:

The hybridization of BRIEF and SVD techniques would be beneficial to cloud users, ICT media hubs, and content creators against piracy, forgery, theft and illegal distributions of multimedia materials. BRIEF and SVD would provide more authenticity, confidentiality, and copy control of multimedia materials.

This study would act as reference material for other researchers who want to conduct further research using the hybridization of watermarking techniques and feature descriptors in securing multimedia contents.

1.6 Organization of the Thesis

This research thesis comprises five chapters ranging from chapter one to chapter five. The background to the study, statement of the research problem, aim and objectives, and the significance of the study are covered in chapter one. Chapter two entails a review of the existing literature related to the research study as well as various definitions, types, challenges, characteristics, merits, and demerits of cloud computing, multimedia, and watermarking. Chapter three encapsulates the methodology, data collection, and performance metrics used to address the challenges faced by previous research and work towards achieving the aim and objectives of the research study. Chapter four gives a detailed explanation of the experimental results obtained, results in discussion, and comparison. Summary, conclusion, contributions to knowledge, recommendations as well as suggestions for future research were drawn in chapter five.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Cloud Computing

Cloud Computing can be known as the metaphor for the Internet, which gives access from anywhere and at any time (Krishnadoss *et al.*, 2021). Cloud computing takes away the physical obstacle for users while providing access to its resources, with users requiring internet connectivity from their end. Internet as a service is one of the resources provided by the cloud to its users. The pay-per-use model is majorly embraced while offering its service to users in the cloud environment.

Cloud computing can simply be referred to as the means of storing and accessing data and programs over the Internet in place of our computer's hard drive. Figure 2.1 shows the typical representation of cloud computing in an internet network, which includes the internet, router, clients, switches, and servers.

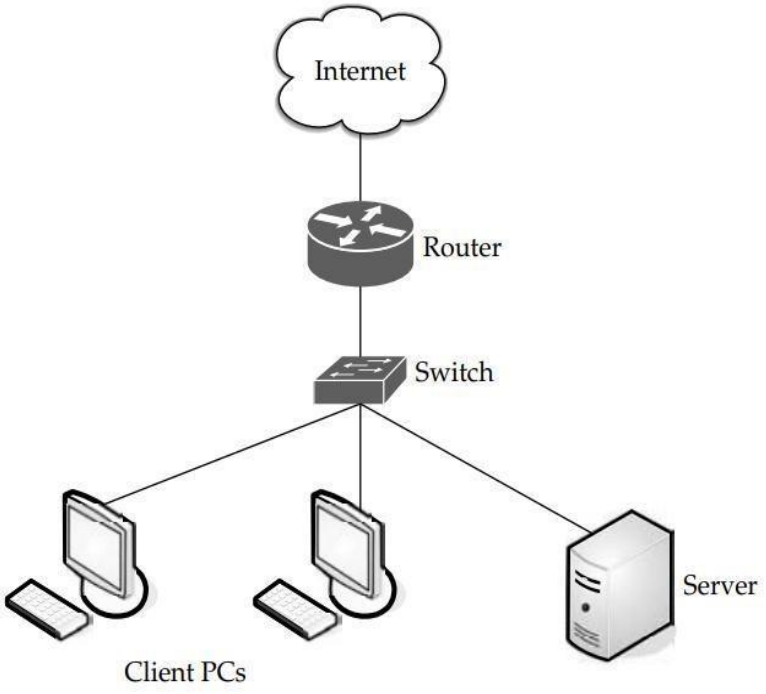


Figure 2.1: Cloud Computing in Internet Network (Rashid & Chaturvedi, 2019).

From Figure 2.1, the internet component of it is a global computer network that provides a variety of information and communication facilities to the cloud, which also consists of an interconnected network using a standardized communication protocol. While the server is a physical computer program or device that provides services. The server is used in the cloud to provide services to other computers and their users. The Client Personal Computers (CPC) provides its client with numerous capabilities like getting to an extensive number of uses without the requirement for having a permit, buying, introducing, or downloading any of these applications and clients can access data anywhere, all they require is to interface with a system usually the internet (Malik *et al.*,2018). Similarly, Switches can also be referred to as computer hardware, switches are used in the cloud for the connection and disconnection of devices. A router has to do with a path of selecting and sending data in a network or between or across multiple networks in the cloud is been handled by the router. Broadly, routing is performed in many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), and computer networks, such as the Internet (Chythanya *et al*., 2020).

According to Salunkhe (2020), cloud Computing is the collection of information technology that support different services that individual uses. In simple terms cloud computing is steering and using data over the internet rather than the computer's hard drive. Cloud computing provides a platform where resources can be shared, rather than steering data on personal physical systems, cloud computing stores data on remote servers. In the work of (Taghipour & Mahboobi, 2020), describes cloud computing as a model for enabling services on-demand network access to a shared pool of configurable computing resources, for example, the networks, servers, storage, applications, and services that can rapidly be provisioned and released with minimal management effort or service.

According to Souley & Adamu, (2017), the use of mobile devices to access and share multimedia content such as images, and video, download software applications, pay online bills, and communicate on the cloud over the internet is increasing with the drastic growth in multimedia technology. However, the inefficiency of mobile devices to hold and handle large size of data due to their limited storage capacity and limited battery life, the need to move and store multimedia data on the cloud becomes necessary for the users.

Considering the work of Sarwar *et al*., (2017), Cloud computing is relatively a new computing model which provides high-performance computational services at a minimal cost. Some famous organizations in the field of IT such as Google, Microsoft, and Amazon have shifted their cloud services over to the internet.

2.2 Evolution of Cloud Computing

In the 1950s, there are large-scale mainframe computers. It was so costly that users could not afford to buy such computers for individual use. For this reason, users started a practice, which was known as “time-sharing”. Time “sharing” allowed many users to use a single computer. It is the same principle as virtualization, which gives a wonderful path toward cloud computing (Namasudra & Pradesh, 2018). In 1960 John McCarthy indicated that like water and electricity, computing can also be sold like a utility. In 1999, the Salesforce Company started distributing the applications to customers through a convenient website. Amazon Web Services was founded in 2002 by Amazon to provide storage and computation services. Around 2009, big companies such as Google, Microsoft, HP, and Oracle began to offer cloud computing services. Nowadays each and every person is using the services of cloud computing in their daily life. For example, Google Photos, Google Drive, and iCloud. In the future cloud computing will become the basic need of IT Industries (Srivastava *et al*., 2019). Cloud Computing is not a new paradigm,

it is an enhancement of various technologies, and it gains popularity day by day because of its various qualities. The evolution of the cloud started with utility computing, grid computing, and then distributed computing (Haris & Khan, 2018). Figure 2.2 depicts various stages involved in cloud computing evolution.

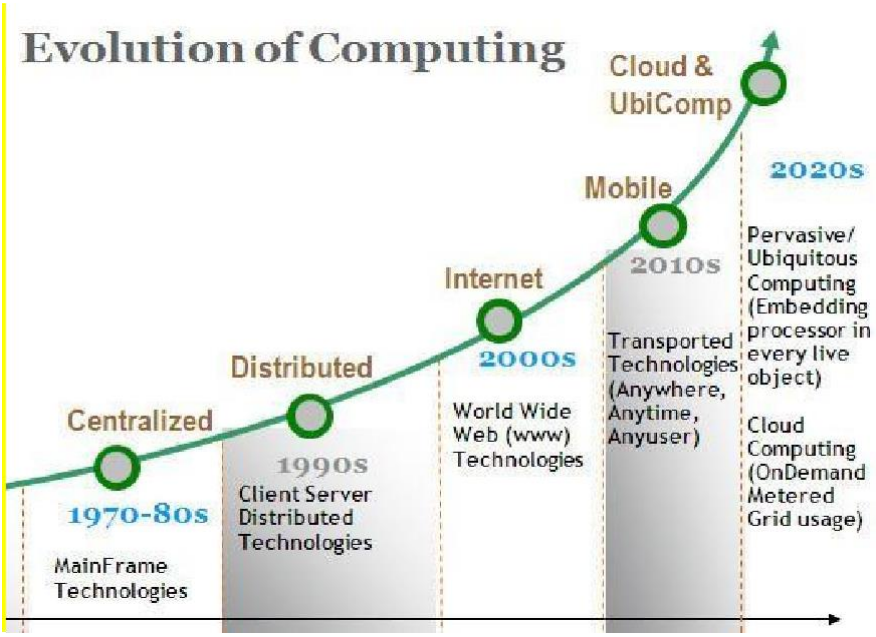


Figure 2.2: Evolution of Cloud Computing (Srivastava & Khan, 2018)

Figure 2.2, encapsulates the five stages of cloud computing evolution ranging from the centralized stage to the cloud & Ubicomp stage. The centralized stage takes care of the mainframe technologies of computing. While the distributed stage of cloud evolution maintains all the aspects of client-server distribution. The internet comes up with the interconnection of global network facilities. Other cloud computing evolution stages include the mobile and cloud Ubicomp.

2.3 Cloud Computing Services and Deployment Models

There are three essential service delivery models available in cloud computing. Figure 2.3 represent a diagram that gives a detailed explanation of the service delivery models

of cloud computing that includes Software as a Service, Platform as a Service, and Infrastructure as a Service.

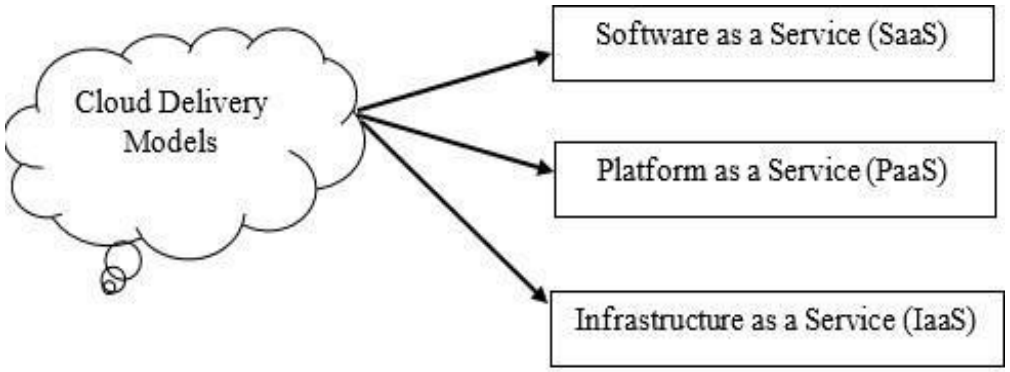


Figure 2.3: Service Delivery Model of Cloud Computing (Ibrahim *et al.*, 2021).

Brief explanations of the three service delivery models of cloud computing are as follows:

2.3.1 SaaS (software-as-a-service): is the software-delivering model used by cloud customers as a pay-per-use service. SaaS is an initial model of cloud services. Examples of SaaS are Google Apps, Salesforce.com, and WebEx (Abdalla & Varol, 2019).

2.3.2 PaaS (platform-as-a-service): is a model which offers the deployment of applications by reducing the cost of buying and maintaining hardware and software. PaaS refers to sharing platform layers and software-layered resources such as operating systems and application-based frameworks. Examples of PaaS are Google Application Engine and Windows Azure (Nazir *et al*., 2020).

2.3.3 IaaS (infrastructure-as-a-service): IaaS provides the consumer with the Computational capabilities of processing, storage, networks, and other computing resources in a centralized location, and allow the consumer to deploy and run their software, which can include operating systems and applications. Examples of IaaS are Amazon Web Services (AWS), Microsoft Azure, and (GCE) Google Compute Engine (Ibrahim *et al.*, 2021; Khan *et al*., 2019).

2.4 Types of Cloud Computing

Cloud computing can be categorized into four main types such as private cloud, community cloud, public cloud, and hybrid cloud as shown in Figure 2.4.

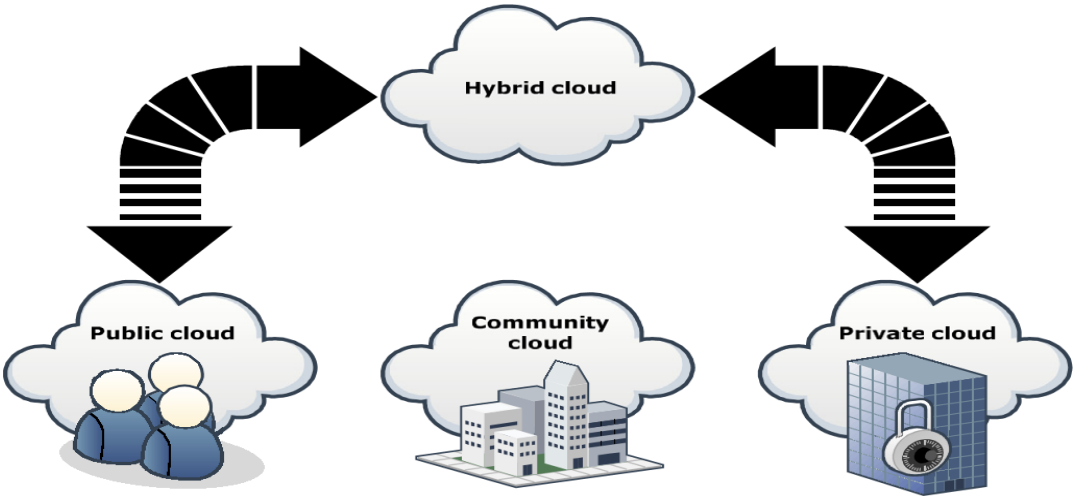


Figure 2.4: Types of Cloud computing (Noor *et al.*, 2018).

From Figure 2.4, private cloud computing resources are deployed for one particular organization. This method is mostly used for business interactions where the computing resources can be governed, owned, and operated by the same organization (Kaur & Bahl, 2018). While the community cloud is an infrastructure that is shared between organizations, usually with shared data and data management concerns. community cloud can belong to a government of a single country and can be located both on and off the premises (Yadav & Sharma, 2019). The public cloud is the type of cloud that is used for B2C (Business to Consumer) interactions. The infrastructure is exclusively used, owned, governed, and operated by the government, an academic, or a business organization (Ali, 2018). Similarly, the hybrid cloud can be used for both types of interactions, Business to Business (B2B) interaction and Business to Consumer (B2C) interaction. Different hybrid cloud and computing resources are bound together by different clouds (Khajanchi, 2019).

2.5 Characteristics of Cloud Computing

According to Rashid & Chaturvedi, (2019), Cloud computing systems satisfy many interesting characteristics that make them promising for future IT applications and services. The National Institute of Standards and Technology (NIST) has defined six essential characteristics of cloud computing systems are described as follows:

(i) **On-demand self-service:** cloud services such as CPU time, Storage, network access, server time, and web applications, can be allocated automatically as required by the consumers without any human interaction. It ensures customers access to the cloud infrastructure without communicating with their cloud provider as needed (Singh & Dhiman, 2021).

(ii) **Cost-effectiveness:** Services provided by cloud service providers are very cost-effective if not free. The billing model is paid as per usage, there is no need to purchase the infrastructure and therefore lowers maintenance costs.

(iii) **Broad Network Access:** Cloud services are available for access from a wide range of devices such as tablets, personal computers, and smartphones. Services can also be accessible from a wide range of locations online (Tanash *et al*., 2019).

(iv) **A Service Measured and Charged for Use:** Cloud Computing automatically measures resources such as Central Processing Unit (CPU), storage, and bandwidth, to enable the user to calculate the invoices automatically (Brahim *et al*., 2017).

(v) **Maintenance:** The system maintenance is been handled by cloud service providers and access is through application programming interfaces (APIs) that do not require application installations onto personal computers and further reduced the maintenance requirements (Kaur & Bahl, 2018).

2.6 Cloud Computing Security Requirement

There are four main cloud computing security requirements, that help to ensure the privacy and security of cloud services. The requirements include confidentiality, integrity, availability, and accountability, which are explained as follows:

(i) **Confidentiality:** Sensitive data such as identities of other users, valuable data, and documents stored on the cloud and the location of the virtual machines, where the target services are executed should not be accessed by unauthorized users (Goumidi *et al*., 2019).

(ii) **Integrity:** Users desire the ability to change, update existing data, or add new data to the cloud. Therefore, data access should be controlled to ensure the safety and integrity of data being stored in the cloud.

(iii) **Availability:** Availability is one of the most critical information security requirements in cloud computing, it is a key decision factor when deciding among private, public, or hybrid cloud. The service level agreement and resources are the most important document between the cloud service provider and the clients (Srivastava *et al*., 2019).

(iv) **Accountability:** Accountability involves verifying the client's various activities in the cloud, accountability is also achieved by verifying the information that each client supplies and logs in various places in the information clouds (Alhenaki *et al*., 2019).

2.7 Merits and Demerits of Cloud Computing Services

Cloud computing is regarded as one of the important computing paradigms for storing, accessing, and providing services to end users and organizations at a minimal cost. Cloud computing has several benefits, that include; easy management, cost reduction, backup and recovery, and disaster management (Jadeja & Modi, 2012).

2.7.1 Merit of Cloud Computing

(i) Easy Management: The maintenance of the infrastructure, hardware, and software is simplified for the IT teams. The applications that are stored and used in the cloud environment are easier to use by service providers compared to when it is used by the organization.

(ii) Backup and recovery: Backups and recovery are essential requirements in the cloud, it is relatively much easier to store the same information on a physical device. The cloud has many techniques and resources to recover any information in the case of any type of disaster(Juman, 2020).

(iii) Cost Efficiency: Cloud is the most cost-efficient method to use, maintain and upgrade, traditional desktop software costs companies a lot, in terms of finances. In addition to license fees for multiple users can also prove to be very expensive for the establishment concerned. The cloud, on the other hand, is available at much cheaper rates and hence, can significantly lower the company's IT expenses (Bhuriya & Sharma, 2019).

(iv) Disaster Management: In case of disasters, an offsite backup is always helpful. Keeping crucial data backed up using cloud storage services, cloud storage services not only keeps data off-site but also ensure the availability of systems for disaster recovery. (Alalawi & Al-Omary, 2020).

(v) Time-Saving: Cloud computing reduces the setup time by dividing tasks among multiple servers simultaneously, the cloud also provides infrastructure, platform, and other facilities that help in running, processing, and saving client time (Juman TP, 2020).

2.7.2 Demerit of Cloud Computing

According to Beri (2015), despite the various advantages of cloud computing, there are several disadvantages of cloud computing. Some of the disadvantages include:

(i) **Requirement of internet connection constantly:** The cloud requires a constant internet connection to provide various services as required by the clients, when the internet connection is down it is impossible to access the services of the cloud offline.

(ii) **Does not work well with a slow internet connection:** Slow internet services such as dial-up connections make it difficult or impossible to use cloud services. This may cause a time-consuming process to use the documents stored on the cloud server.

(iii) **Lesser Security:** The use of the public cloud often leads to lesser security and confidentiality of information in the cloud, this could be violated when unauthorized access occurs. For example, hackers, can damage the data or misuse the data (Alhenaki *et al.*, 2019).

2.8 Multimedia in Cloud Computing

Digital multimedia such as text, images, audio, and videos play an important role in applications such as news reporting, intelligence information gathering, criminal investigation, security surveillance, and health care. However, this trustworthiness could no longer be granted since users can easily manipulate, modify, or forge digital content without causing noticeable traces using low-cost and easy-to-use digital multimedia editing software tools. The Cloud computing paradigm is very useful for multimedia applications over the internet. Therefore, digital multimedia authentication has become an important issue (Ashraf *et al.*, 2018).

Multimedia applications require digital media, computing power, storage capacity, speed of data transfer, reduction in power consumption, efficient algorithms, and cost. This could prompt cloud users to store rich multimedia documents and easily access the document from the cloud

(Bhavikatti & Banakar, 2019). Cloud resources are in high demand because of the following key reasons:

(i) **Hardware Limitations of Mobile Devices:** Handheld mobile devices such as mobiles, tablets, and notebooks are of small size, economical, and lightweight but carry limited processing power, memory size, and limited battery life. There is a huge gap between the processing speed of a cloud server and a mobile device. These limitations of mobile devices raise the demand for cloud computing for accessing, storing, and processing rich multimedia content.

(ii) **Extreme Demand for Resources:** Multimedia content such as videos, images, audio files, presentations, multimedia mail, internet gaming, and sensor networks are dominating today's internet traffic and this trend is going to increase in the future. These media contents require storage and computing at a large scale (Nazir *et al*., 2020).

2.9 Challenges in multimedia cloud computing

Multimedia processing in a cloud imposes great challenges. Several fundamental challenges of multimedia computing in the cloud are highlighted as follows.

i. **Multimedia and service heterogeneity:** There exist different types of multimedia and services, such as video conferencing, photo sharing and editing, multimedia streaming video and audio, image search, image-based rendering, video transcending and adaptation, running sensors, and multimedia content delivery, the cloud shall support different types of multimedia and multimedia services for millions of users simultaneously (Sahu & Pandey, 2018).

ii. **Device heterogeneity:** As different types of devices, such as TVs, personal computers (PCs), and mobile phones, have different capabilities for multimedia

processing, the cloud shall have multimedia adaptation capability to fit different types of devices, including a central processing unit, memory, storage, and power.

iii. **Power Consumption:** The expanding scale and density of data centres has made power consumption an imperative issue. therefore, a recent phenomenon has been the astounding increase in multimedia data traffic over the Internet, which in turn is exerting a new burden on energy resources (Yang *et al*., 2020).

iv. **Security:** Security is one of the crucial concerns in the cloud, which obstructs the growth of cloud computing, sensitive and confidential multimedia data content requires strong security techniques to protect users' data from hackers (Suyel *et al*., 2021). One of the best approaches to overcoming the security challenges in cloud computing is the use of the digital watermarking technique.

2.10 Digital Watermarking

Digital Watermarking is the process of embedding information into digital media, such as text, images, audio, and video. Thaiyalnayaki & Devi, (2018), define watermarking as a group of bits inserted into a digital data file that identifies the file's copyright information. Usually watermarking has been used in currency notes, government documents, passports for security features, and stamp papers for legal purposes. Digital multimedia contents that include text, image, audio, video and animated applications need to be safeguard from stealing, eavesdropping, tempering and hacking (Uma & Sumathi, 2017).

In the work of Tanwar, (2018) describe digital watermarking as the process of inserting secret information, related to the identity of the owner and the source, into the original digital data such as image, text, audio, and video, this secret information is known as a watermark.

Digital watermarking is a security technology that embeds signals and secret information called watermarked within digital media content such as images, audio, and video (Souley & Adamu, 2017). It ensures security, privacy, and ownership authentication of the media content being watermarked. The idea behind watermarking is related to steganography. Steganography is defined as secret writing, which is used for secret information over a long-time history. Digital watermarking is used to hide labels or marks on media content which could later be detected and extracted by an authorized user to protect product copyright or media data integrity.

2.11 Background of Digital Watermarking

With the rapid development of the World Wide Web and the ease of access to the Internet, multimedia data such as images, audio, and videos, can be accessed, downloaded, copied, modified, and redistributed easily. On one hand, it provides a way to access useful information from anywhere instantly and easily, but on the other hand, it has created problems for intellectual property owners. For instance, the data can be copied and redistributed illegally, without any visibility between the original and copied data, especially for the end user. It is also difficult to track the difference in the origin of the illegal distribution of the copied material. Due to these illicit distribution industries suffer enormous losses each year. Therefore, some measures must be taken to avoid further unlawful distribution or to provide a method to claim ownership. Additionally, sensitive information such as confidential documents, military documents, and medical documents can be modified or altered before reaching the intended user. Hence, the expected end user must be capable of identifying the authenticity of received data. To address such issues, watermarking is proposed as an intended or prominent solution (Imran, 2016). Figure 2.5 represents the three essential requirements of digital watermarking techniques that include the host image, watermarking embedding, and watermarking extraction.

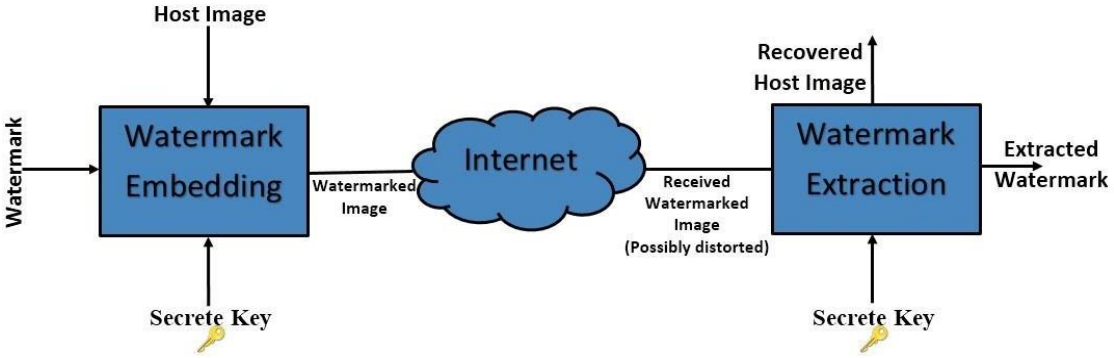


Figure 2.5: General Framework of digital Watermarking (Imran, 2016).

The three essential requirements of digital watermarking consist of the host image, watermarking embedding and watermarking extraction. Other requirements including the internet and secret key are explained as follows:

(i) Digital (Host) Image Watermarking: Digital image watermarking is the process of inserting essential information/logo under an image that can be used to validate its authenticity or the identity of its owners. The straightforward manipulation of data constitutes a real threat to information creators, and copyright owners (Bala & Pal, 2021).

(ii) Watermark Embedding: Watermark embedding is the process of embedding or inserting the message or content into the original or host image. The embedding should be done in such a way that it satisfies all the properties like security, confidentiality, reliability, availability, integrity, authenticity, and traceability and should ensure legitimacy (Selvakumari & Jeyaraj, 2018).

(iii) Watermarking Extraction: The yield of the embedding procedure that is watermarked will be the contribution of the extraction process. The kind of key relies on the sender whether it is open or private. Utilizing a specific watermarking extraction method, the original information is recovered from the watermarked information (Kaur, 2017).

2.12 Applications Area of Digital Watermarking

Digital Watermarking can be applied in numerous areas such as Copy Protection, Copyright Control, Broadcast Monitoring, Electronic Voting Systems, Remote Education, and Digital fingerprinting. Other areas in which digital watermarking can be applied are medical applications, tamper disclosure, hidden annotations, authentication, and covert communication. (Agarwal *et al.*, 2019).

Figure 2.6: Applications Area of Digital Watermarking Techniques (Wazirali *et al.*, 2021).

The application areas of digital watermarking from Figure 2.6, are described as follows:

(i) **Copy Protection:** The main goal of the watermarking application is to provide copyright protection to digital information by hiding secret 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 (Alshoura *et al.*, 2021).

(ii) **Electronic Voting System: -** The Internet has spread all over the country from big towns to small villages. Electronic voting helps to carry out elections, keeping the security aspect into consideration.

(iii) **Broadcast Monitoring: -** Broadcast Monitoring is a verification technique that verifies and ensures whether the data that was supposed to be broadcasted has been broadcasted or not. Over the years it has been seen that the availability and accessibility of media content have increased exponentially (Rawat *et al.*, 2016).

(iv) **Copyright control: -** Watermarks can also be used for copy prevention, and copy control, and can prevent illegal duplication of digital data. Replication devices can detect watermarks and report copying and also prevent illegal copying (Ji *et al.*, 2020).

(v) **Remote Education: -** Lack of teachers poses a big problem in small villages. Smart Technology needs to be adopted for distance learning. In this case watermarking plays its role in authenticating the transmission of study materials over the internet.

(vi) **Digital Fingerprinting:** Digital fingerprinting is a technique used to detect digital content ownership. Fingerprints are unique to the digital data owner, a single digital content may therefore have different fingerprints because it relates to different users (Lande, 2019).

2.13 Features of Digital watermarking

The features of digital watermarking play an important role in the development of a watermarking system for different applications (Kumar *et al.*, 2020). There are several features of digital watermarking as shown in Figure 2.7.

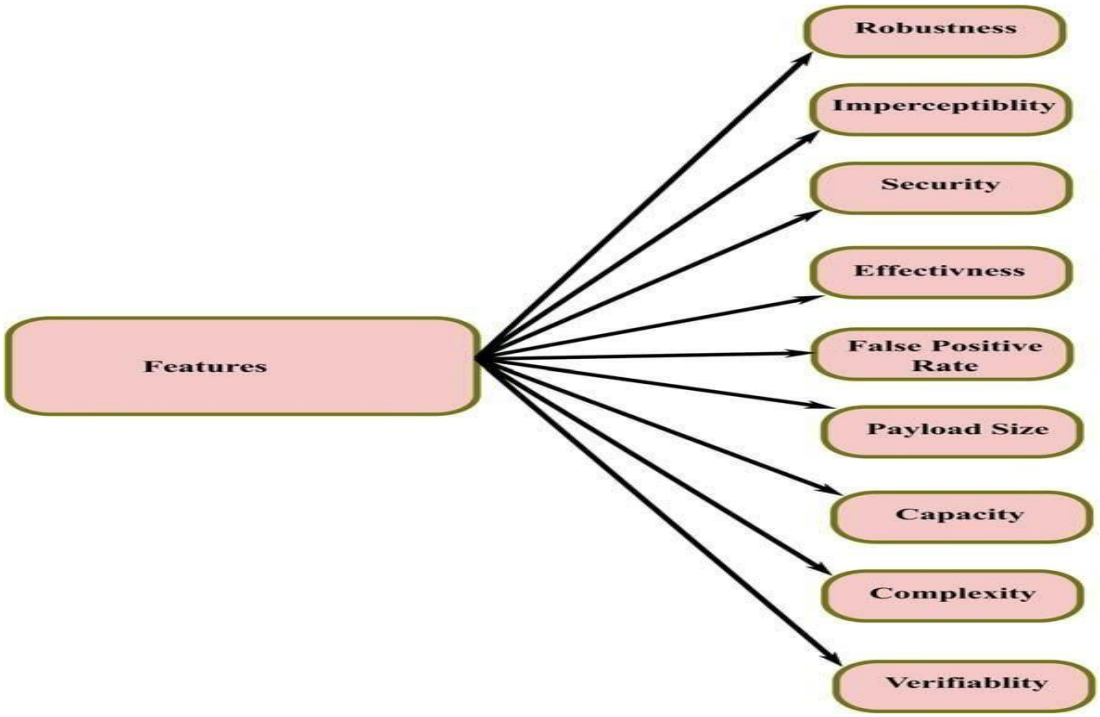


Figure 2.7: Features of Digital Watermarking (Kumar *et al*., 2020).

Figures 2.7 represents various features of digital watermarking such as robustness, imperceptibility, capacity, security, verifiability, fragility, and cost. Other features of digital watermarking include the false positive rate, complexity, effectiveness, and payload size.

(i) **Robustness:** The robustness feature of digital watermarking refers to the survival of embedded watermarks against any image processing, operations, and attacks. These attacks may include spatial filtering, copying, cropping, scaling, translation, compressing, and rotation either intentionally or unintentionally (Arora, 2018).

(ii) **Imperceptibility:** The imperceptibility feature indicates that the digital watermark cannot be seen by the human eye, the watermark should be invisible. The quality of the content should be maintained after embedding a watermark on the media content (Jaiswal & Ravi, 2018).

(iii) **Security:** Unauthorized users are not in a position to detect and neither retrieve nor change the embedded watermark. The security feature indicates that irrespective of targeted attacks, the inserted digital watermark cannot be removed. Watermarking security can be explained as a way to provide secrecy, ownership, and protection of data (Embaby *et al*., 2021).

(iv) **Capacity:** The capacity or volume that characterizes the number of bits or the greatest data which can be inserted into the host image (Madhavi *et al*., 2019).

(v) **Verifiability:** Through the watermark, there should be a trace of evidence regarding the ownership of copyright-protected data. This helps in verifying the authenticity of any digital data and even controls its unlawful copying (Kumar *et at.,* 2020).

(vi) **Fragility:** The fragility of the watermark refers to its sensitivity towards any slightest modification tried. The foremost property of a fragile watermark is that whenever it faces some illegal modification, it becomes undetectable (Kadian *et al.,* 2021).

(vii) **Cost:** The cost of any watermarking system is generally the computational cost involved in the whole watermarking process which involves watermark embedding and watermark extraction.

2.14 Attacks on Digital Watermarking

Watermarking attacks on digital objects fall into two categories, consisting of both intentional and non-intentional attacks (Wazirali *et al.,* 2021).

2141 Intentional Attacks

Intentional attacks typically involve the use of computer coding or other technical devices, which are designated to cause some unwanted issues. Meanwhile, non-

intentional attacks include software bugs that occur during the programming of a computer system or system configuration.

(i) **Forgery Attack:** In this type of attack the hacker assimilates the watermark into the cover image without extracting the original watermark. The unique threshold values are sent as secret keys to the receiver to make the final image resistant to forgery (Puppala *et al.*, 2020).

(ii) **Eavesdropping:** This type of attack is known as snooping or sniffing attack where the attacker takes the advantage of insecure communication among devices for gaining access to data when is being received or sent by the users.

(iii) **Active Attacks:** The hacker intends to remove the watermark or simply make it undetectable. The hacker aims to distort an embedded watermark beyond recognition. An example of active attacks is copyright protection, fingerprinting, and copy control (Agarwal *et al.*, 2019).

(iv) **Passive Attacks: -** In passive attacks, the attacker does not try to remove the watermark but simply attempts to determine if a given mark is present or not. Protection against these kinds of attacks is of utmost importance in secret communications (Kumar, 2018).

(v) **Cryptographic Attacks:** Gaining information about what type of security scheme is used during watermarking by collecting security information, an attacker can remove the watermark information or attempt to change the state of watermarking information. This turns to mislead the original owner of the data by modifying the information about the original files (Navneet & Shailendra, 2013).

(vi) **Geometric Attacks:** Rotation, scaling, and cropping are three common geometric attacks. A small geometric attack can lead to the problem of watermarking desynchronization, resulting in the watermark being unable to be correctly extracted, a

considerable number of watermarking algorithms have relatively weak resistance to geometric attacks (Yu *et al.,* 2019).

(vii) **Protocol Attack:** The attacks which come under this category, do not damage the embedded data. Three types of Protocol attacks are invertible attack, Copy attack, and ambiguity attack. The watermark should be noninvertible and should not be copied, a watermark is invertible when the attacker removes the watermark from the host data and pretends to be the owner of the data (Begum & Uddin, 2020).

(viii) **Copy Attack: -** this type of attack is in the form of a protocol attack; the watermark is not destroyed. Instead, the attacker estimates the watermark from host data and copied it to available data.

2.14.2 Non- Intentional Attacks

(i) **Removal Attack: -** Removal attacks aim to remove the watermarking data from the watermarked object. Based on these attacks, watermarking represents an additional noise of signals, which are presented within the host signal.

(ii) **Compression: -** this type of attack represents an unintentional attack, which emerges repeatedly through various applications that involve multimedia. In particular, the whole compressed objects are distributed throughout the Internet (Wazirali *et al.,* 2021).

2.15 Digital Watermarking Techniques Based on Document Types

Digital watermarking techniques can be categorized into four main types. These are as follows:

i. **Text Watermarking: -** Text watermarking is an approach for text documents and copyright protection. Digital watermarking for text documents is primarily classified into three types:

Line shift coding - This vertically shifts the location of text lines to encode the document. While the shift coding is horizontally shifts the location of words to encode the document. Similarly, feature coding chooses certain features and alerts those selected features.

ii. **Image Watermarking: -** Image watermarking is to obscure the copyright information into the image format and extract the particular information for the author's ownership. The process of image watermarking includes embedding the watermark into the original image and extracting the watermark from the image where the copyright information is hidden (Sasi & Arul, 2019).

iii. **Video Watermarking: -** This involves embedding cryptographic information derived from frames of digital video into the video itself.

iv. **Audio Watermarking: -** In this method, an electronic identifier is embedded in an audio signal. Some authors proposed the use of text or images to be embedded in the audio file such that any audio file could be analysed for a possible recovery (Thaiyalnayaki & Devi, 2018).

2.16 Merits and Demerits of Digital Watermarking

There are various advantages as well as disadvantages of digital watermarking. Some of the advantages and disadvantages are shown in 2.16.1 and 2.16.2 (Agrawal, 2015).

2.16.1 Merit of Digital Watermarking

(i) Digital watermarking is the potential solution for content authentication, protection of multimedia content, copyright management, temper detection, and protection of ownership rights against any unauthorized copying or redistribution of multimedia content (Kumari, 2017).

(ii) Digital watermarking can easily be used to detect copyright violations, piracy, counterfeiting, and temper detection of digital content.

(iii) Digital watermarking is a secure technique that concealed information while being transferred through a channel. Digital watermarks use a key to secure digital multimedia and can only be removed by authorized users, this is done to prove the ownership of the data (Anil *et al.*, 2020).

2.16.2 Demerits of Digital Watermarking

(i) Digital watermarking such as images, video, and audio disappears when being influenced and any executed operation like compression, resizing and rotation reduced the quality of the watermarking significantly (Garg & Kishore 2020).

(ii) Low website connection can attract attention or could create avenues for hackers to compromise the process of watermarking extraction. Other disadvantages include process overhead, time-consuming, and interference with digital content (Soni & Kumar 2020).

2.17 Types of Digital Watermarking

Generally, Digital watermarking can be categorized as either visible or invisible watermarking (Sasi & Arul, 2019). Figure 2.8 and 2.9 presents the sample images of both visible and invisible watermarking

(i) **Visible watermarking:** this is a type of watermark that can be seen by everyone who is seeing the data object. Visible watermarking is mostly used for copyright protection. This technique can be highly fragile if the watermark is placed in a non-significant part of the image, where it can be covered, cropped, or removed (Srivastava *et al.*, 2021).

Figure 2.8: A Sample of visible image watermarking (Srivastava *et al.*, 2021).

(ii) Invisible or Hidden watermarking: this is a type of watermark that provides a backup facility in case the visible watermark fails. Invisible watermarking can be fragile or robust depending on how and where the watermark is embedded in the image. Therefore, invisible watermarking is commonly used for both copyright and authentication applications (Madhavi *et al.*, 2019).

Figure 2.9: A Sample of Invisible Image Watermarking (Madhavi *et al.*, 2019).

2.18 Domains of Digital Watermarking Techniques

The domain of digital watermarking techniques can be divided into three groups such as spatial domain watermarking technique, frequency domain watermarking techniques, and hybrid domain watermarking techniques (Pal *et al.*, 2018).

2.18.1 Spatial Domain Watermarking Technique

The spatial domain watermarking technique can also be referred to as the pixel domain technique, in spatial domain watermarking, a watermark is embedded directly into the pixel values of the host image. The spatial domain technique is conceptually easy and has

very less computational complexities (Agrawal, 2015; Bala & Pal, 2021). Some of the algorithms that work on the spatial domain are Least Significant Bit (LSB), Spread Spectrum Modulation (SSM), and Patch Work Algorithm (PWA).

(i) **Lease Significant Bit (LSB):** The LSB is the simplest spatial domain watermarking technique, the main advantage of LSB method is easily embed in cover images, it provides high perceptual transparency when the watermark is embedded, LSB does not degrade the quality of the image (Rashid, 2016). LSB watermarking is very sensitive to noise, the method implemented gives the idea about the influence of various noise in LSB watermarking by using an LSB algorithm encrypted secret image gets embedded into the original image (Joseph & Rajan, 2020).

(ii) **Spread-Spectrum Modulation Based Techniques (SSM):** Watermarking algorithm embeds information in the context of image watermarking and when applied to the context of image watermarking, it embeds message by combining the cover image with a small pseudo-noise signal modulated by the added watermark (Rawat *et al.*, 2016).

(iii) **Patch Work Algorithm (PWA):** In the patchwork algorithm an image is divided into two patches X and Y where patch X is brightened by some factor alpha while patch Y is darkened by the same factor. The watermark is embedded in these patches using some encoding technique and then extracted by using the same factors (Garg & Kishore, 2020).

2.18.2 Frequency Domain or (Transform Domain) Watermarking Technique

Frequency domain-based watermark techniques do not embed the watermark image directly into the host image. Rather, these techniques consider the frequency coefficients of the watermark image and host image. Some of the popularly used frequency domain-

based techniques are Discrete Wavelet Transforms (DWTs), Discrete Fourier Transforms (DFTs), Discrete Cosine Transforms (DCTs), and Singular Value Decomposition (SVD) (Singh *et al.,* 2020). In the frequency, domain modification is done on certain frequency components of the images, and algorithms (Pal *et al.,* 2018).

(i) Discrete Wavelet Transforms (DWT)

Discrete Wavelet Transform is a modern watermarking technique that is frequently used in digital image processing and image compression. The main advantage of DWT its understands the Human Visual System (HVS) more closely than other watermarking techniques (Rashid, 2016).

(ii) Discrete Cosine Transform (DCT)

The DCT transform is mainly used to compress the data or image, which can convert the signal from the spatial domain to the frequency domain, and has good performance of de-correlation. DCT is lossless and creates good conditions for the following quantization. For example, DCT is used to inverse transform after quantization coding to restore the original image information at the end of receiving. DCT is widely used in the field of image analysis (He & Hu, 2018).

(iii) Discrete Fourier Transform (DFT)

The Fourier transform is the most basic transform, many problems can be processed in the spatial domain and transform domain with DFT at the same time. The DFT can be used to represent discrete information since the image is stored in the computer in digital form (Su *et al.,* 2019).

(iv) Singular Value Decomposition (SVD)

SVD is a powerful and convenient matrix decomposition, SVD works under frequency domain watermarking techniques. SVD is regarded as the

most important technique in terms of protection and usability. It is also applied in the spatial domain, with small changes implemented on singular values enabling incomprehensible features (Şahin & Guler, 2021).

2.18.3 Hybrid Domain Watermarking Technique

Hybrid domain watermarking techniques combine two or more transform domain algorithms. These include DCT and DFT, DCT and DWT, DCT and SVD, DFT and DWT, DFT and SVD, DWT and SVD, and a combination of DCT, DFT, and DWT (Begum & Uddin, 2020).

2.19 Related Studies

Cloud Computing is a dynamic term that provides dispute-free data outsourcing facilities which prevent the user from the burden of local storage issues. However, the biggest issues to be focused are on providing secure and reliable data and other multimedia content in a cloud archive over unreliable service providers (Khajanchi, 2019). One of the challenges in cloud computing services is security issues. For example, broken authentication, compromised credentials, account hacking, data breaches, lack of expertise, password security, and cost management are on the rising. With the capabilities of super-computing and mass storage provided by cloud computing, cloud security still remains a challenge or issue in securing digital content, which is in essence the trust management between data owners and storage service providers. Cloud security is the security problem of virtual storage in cloud computing.

The classic challenges of data storage turn into a social problem in the selection of data storage services for data owners, which reflects human social activities onto the Internet in miniature (Ramesh *et al.*, 2012). Data owners care about whether the provider of data storage service will use their data, or reveal it to a third party without authorization.

Therefore, trust management between data owners and storage services providers is an essential problem in cloud security, which demands an effective stipulation of data usage.

The literature of Mohammed *et al*. (2021) presents an authentication technique for digital images, digital images are transmitted through insecure mediums such as the internet and computer networks of various kinds, and the applications may require a high level of security techniques such as Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT) were used to solve the problem of insecurity. The essential requirements for designing an efficient watermarking system are robustness, imperceptibility, and capacity. However, despite the use of the aforementioned techniques fulfilling all of the requirements concurrently is nearly impossible. The researchers suggested that feature work can be expanded by combining different techniques to satisfy the critical requirements as outlined in this research. Additionally, researchers should concentrate on enhancing the robustness, imperceptibility, and security of data and multimedia content.

Cryptography, such as digital signature and hash functions, was used by Vybornova, (2020), to secure a video from modification, replication, deletion, insertion, and replacement of frames or objects in frames. Such systems do not provide information about the type of attack, and video is considered inapplicable as evidence. An experimental study on the method's quality and efficiency was conducted. Vybornova, (2020) proves that the experimental results based on the method used were suitable for solving authentication tasks. This research suggested the development of an algorithm for the differentiation of attack types, and enhancement of the watermark robustness against compression by developing an improved detector for amplitude peak and robustness

against various types of possible geometrical attacks, such as cropping and rotational attacks.

Considering the work of Ray and Roy, (2020) proposed the use of Singular Value Decomposition (SVD) and Advance Encryption Standard (AES) techniques for copyright security and safety of bank cheque images. During digital communication intruders or attackers may be observing the data spreading through the channel and can apply active and passive attacks on the bank cheque images. To overcome exploitation, this method applied SVD-based image watermarking for copyright protection and 256-bit key AES encryption for security services. However, this survey paper stands beneficial with significant insight for beginners as well as proficient researchers working in information security and other domains requiring robust and secure watermarking. In future endeavours, various other applications of data-hiding techniques can be explored.

Thaiyalnayaki and Devi, (2018) presented that cloud computing looks like a big black box with its content invisible to the clients, clients have no idea or control over what happens inside the cloud. This may result in the violation of confidentiality and integrity of the system due to a lack of assuring security, and privacy guarantees become the main barrier to further deployment of cloud-based image processing systems. To overcome these challenges, the techniques of robust reversible watermarking and RSA digital signature, Singular Value Decomposition (SVD), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) techniques were implemented on cloud architecture to check the robustness of the watermarked data, the performances of the techniques were analyzed with Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) value. The researcher proposed a solution based on different watermarking techniques and methods to enhance privacy and security.

The growing rates of data hacking which has made access to private data easier have raised alarms for users to secure their data with better algorithms (Gill & Varma, 2016). A thorough analysis of watermarking techniques was carried out and found that all the watermarking techniques developed were some advancements of the conventional techniques. Furthermore, the drawbacks of the techniques in this research were resolved in their newly proposed techniques as they were all robust against one or the other attacks when MATLAB software is used. The outcome shows that the best techniques to protect data against all possible attacks are Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) techniques.

Every data (raw and processed) available on the internet needs to be protected from forgery and theft; data in plain text, images, videos, and audio were no longer safe, as such watermarking has given some certain degree of authenticity and security to data owners (Sarwar *et al.,* 2017). Their research work gave evidence of the reliability of watermarking techniques that ensure the provenance of data security and integrity and other important issues such as data reliability, robustness, distortion, and capacity were also taken into consideration, however, some of the techniques used failed to solve the problem to the optimal level. However, Souley & Adamu, (2017) and Uma & Sumathi, (2017), were able to provide a strong authentication medium for media and enhanced its integrity and security protocol, using digital signature and robust reversible watermarking techniques respectively. They suggested that future research should implement this same technique on video watermarking technique and evaluate the performance of the system with other existing techniques by other researchers.

Sarwar *et al.* (2017) in their research work, used visible and invisible watermarking techniques to secure shared data objects in cloud computing. The Major challenges of

shared data objects in a distributed environment are piracy and security. By adopting these techniques, shared data objects in the cloud can be safe from malicious attacks that may change or lose the real ownership of the data objects. The experiment was performed by using both visible and hidden watermarking and the experimental results demonstrate the efficiency and reliability of the proposed technique. This research work suggested that future work should include some other techniques that would ensure the trustworthiness of shared data objects among different cloud computing environments simultaneously.

Bahrami and Tab, (2016) propose the use of a new robust watermarking algorithm based on SURF features and block classification, to enhance robustness, stability, imperceptibility, time complexity, and real-time performance and also improved the method to cope with most attacks. By using this proposed method on the three challenges the drawbacks can be overcome. First, select a proper region for watermarking particularly, in videos that suffer from redundancy. Second, the issue of synchronization problems in the watermark detection from cropped and rotated video are sometimes ignored or not emphasized mainly which is resolved by employing the Speed Up Robust Feature (SURF). Finally, based on the advantages of this scheme, it will provide ways by which digital media could be safe from illegal duplication. There are still some issues left for future work to reduce the time complexity to apply the proposed method for real-time video watermarking by reducing information overhead.

In the work of Kumar and Singh, (2019) thorough research on the field of reversible watermarking techniques on several aspects of security challenges faced by data in computing is secure by the use of reverse watermarking and steganography. In this research study, the development of packet sender and receiver module was made and able to achieve more security, better performance, flexibility, and reliability and can be applied

to almost all types of images in a cloud computing environment. Client-server model, Ip4 addresses, port, java socket programming, and MATLAB tools were used. This research work would be capable of providing security as in the proposed work, the reverse watermarking technique has been integrated. The proposed research work would be better than the existing research.

Sowmya *et al.*, (2021) proposed the use of a nested watermarking technique to secure digital contents that suffer from an infringement of copyrights, data piracy, and illegal modification. Sowmya *et al.* (2021) further stated that in the proposed system java was used to implement the watermarking algorithm. A nested watermark is encrypted before embedding into the main digital content and the proposed technique was able to protect sensitive information against illegal manipulation by hackers. The researcher recommended that future studies should consider using the same technique and proposed the use of metrics such as PSNR, BER, and MSE to evaluate the performance results of nested watermarking techniques.

Srivastava *et al.* (2021) suggested the use of Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) techniques for providing high imperceptibility, strong robustness, more security, and high capacity. This research work focuses on providing strong robustness and high capacity. The embedded watermark does not distort the quality of the original image. Lots of research has been conducted to design solutions for providing high imperceptibility, strong robustness, more security, and high capacity. Hence, this combined method was used with pixel modification techniques, which enhances the capacity, robustness, and imperceptibility, and reduces the total execution time. Four parameters are analysed (PSNR, NC) which shows the performance improvement of the proposed method. In the feature, the researcher suggested that the same method can be used and the same approach can also be implemented for video watermarking.

Soualmi *et al*.(2020) proposed a new watermarking approach that considers special features of medical images, tempering medical images could lead to wrong interpretation by the physician which could lead to serious consequences. This paper proposes a new watermarking approach to ensure medical image authenticity, using Min Eigen value features, chaotic sequence, and Quantization Index Modulation (QIM) in the spatial domain. The proposed technique is blind which means that the data embedded could be extracted only with the key used in the embedding phase without needing the original image or the watermark. Normalized Correlation (NC) and Bit Error Rate (BER) are used to test the performance of the proposed techniques and the results demonstrated high robustness against attacks used in experimentation. The researcher suggested that future works should attempt to improve this method in terms of data payload and robustness against other attacks.

Digital images are widely communicated over the internet. The security of digital images is an essential and challenging task on a shared communication channel. Various techniques are used to secure the digital image, such as encryption, steganography, and watermarking. These are the methods for the security of digital images to achieve security goals, confidentiality, integrity, and availability (CIA) (Razzaq *et al.*, 2017). The researcher further proposed the use of blended image security techniques to ensure the confidentiality, integrity, and availability of digital images. Experimental results obtained by the proposed method were promising. The researcher suggested that in the future, the secret keys can also be applied in steganography.

Fita and Endebu, (2019) proposed the use of Singular Value Decomposition (SVD) techniques for securing multimedia content and data protection, digital multimedia is undergoing drastic changes in information communication technologies. This research

proposed an algorithm for colored digital image watermarking techniques based on SVD. Covers embedding, watermarking extraction algorithm, and some robustness tests while both host and watermarking images are colored (Fita & Endebu, 2019). The quality of the watermarked image is evaluated using Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). The experimental result is simulated with the software MATLAB R2017b Version and the experimental result shows that the algorithm is robust against geometric attacks.

Vo *et al.* (2017), carried out research work to merge Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) techniques for copyright protection of stereo images. In today's forgery world, digital images can easily be manipulated and modified by software tools, while communicating the data over insecure channels such as the Internet. Therefore, the protection of ownership and the prevention of unauthorized tampering with stereo images have become urgent matters. The solutions to these problems can be known as cryptography and data hiding. In the cryptography technique, data is transformed into meaningless form and is transmitted to the receiver. Conversely, data hiding conceals secret information into carrier objects to avoid suspicion from adversaries. In this research study, a DCT-SVD-based, robust, hybrid image, watermarking scheme for stereo image copyright protection has been proposed.

The literature of Selvakumari and Jeyaraj (2018), stated that watermarking of the medical image greatly assist in authentication for safe data storage and transmission of an image in databases. Though perfect methodologies for indexing the medical images would provide quick retrieval performance. This problem has not been perfectly addressed in the literature. In this paper the researcher carries out image watermarking steps for indexing medical images, also an experiment is carried out on embedding and extraction

of both visible and invisible watermarking algorithms. The result of the research work obtained is based on the need for a watermarking algorithm that shows high embedding as well as extraction performance for reaching the medical image indexation need. It is being concluded that in the implementation of a visible and invisible watermarking method for embedding purposes, LBP shows better performance in case of extraction purposes, IWT shows better performance where LBP shows the least. Therefore, there is a need for an algorithm that shows better performance in both embedding and extraction.

According to the research work of Amiri (2022) the researcher mentioned watermarking is placing a message hidden in the media without any form of alteration. It is also mentioned that transform (frequency) domain-based watermarking has been most used due to its advantage over the spatial domain. In this case, a solution was proposed, by providing a scheme with a robustness of the cover image to differentiate damages, and also maintain the unnoticeable of the watermarked image. In other to accomplish this goal the researcher makes use of three transforms with a differential evolutional algorithm. For further research work, the paper concluded that the security of the proposed method can be increased in the embedding which was obtained.

Reviewing the work of Meg (2022) titled Architecture of a fake news detection system combining digital watermarking, signal processing, and machine learning. The researcher talked about the present world in which much fake news and information is been circulated which is becoming a threat to people and different sectors. A solution was proposed, by designing an architecture to detect fake news on the social media platform. It is concluded that the main goal of the research work is to create a tool that makes use of digital watermarking techniques, machine learning, and digital processing. For future work, it has been stated that this article is an initial step toward the goals that the

researcher mentioned. A system detector that proved a merge of data hiding, machine learning and the multimedia forensic system can be created to effectively detect fake news.

To verify the performance of the proposed scheme, the experiments are implemented in the MATLAB platform on the cover stereo image and were evaluated using Peak Signal Noise Ratio (PSNR) and Bit Correlation Error (BCR). And the experimental results showed that the proposed scheme can resist different types of image-processing attacks.

The summary of related work that is based on the problem addressed, techniques used, findings, and limitations of related works are presented in Table 2.1.

Table 2.1: Summary of the Related Works

S/N	Author/Year	Title	Problem Addressed	Approaches Used	Findings	Limitations
1	(Savaridass *et al.*, 2021)	Digital Watermarking for medical images using DWT and SVD technique	In the medical field, confidential dragonize information is recorded and stored digitally and transmitted. The process of transferring security and authenticity is the main challenge faced in the medical field	The researchers employ hybridized techniques by combining the Discrete Wavelet Transform and Singular Value Decomposition	The medical image has proven to be robust to attacks such as salt and pepper noise, Gaussian noise, and filtering attack.	The paper does not cover watermarking schemes for color images and video.
2	(Singh *et al.*, 2019)	Suitability of Singular Value Decomposition for Image watermarking	The extensive use and exchange of digital images via the internet prompt the need for establishing authorship of the image	The Singular Value Decomposition (SVD) for watermarking digital images	A comprehensive analysis to understand the ability and limitation of SVD techniques in hiding information.	other watermarking scheme algorithms are not considered in this thesis
3	(Wang *et al.*, 2021)	A Multi BRIEF descriptor stereo matching algorithm for binocular visual sensing for fillet welds with indistinct features	The similar attribute or features of the surface of a weldment has made the stereo machine operation in binocular vision difficult	The paper proposes the use of a Multi BRIEF descriptor stereo matching algorithm.	The stereo-matching output shows that method used has an advantage in minimizing and obtaining more matched feature points in comparison to the SURF description	Situations such as distinct features and similarity disparity of binocular vision are not looked at.

4	(Wang *et al.*, 2019)	GA-ORB: a new efficient feature extraction algorithm for multispectral images Based on Geometric Algebra	Feature extraction and multispectral images are very challenging due to the fact that information is encapsulated in both the spectral and spatial space.	The use of Geometric Algebra – ORB for feature extraction	The result gotten from the experiment shows the GA-ORB approach outperforms some of the previous techniques with respect to robustness in extraction and matching	The research work does not focus on the various application of multispectral images based on the GA-ORB approach
5	(Tan *et al.*, 2019)	Distinctive accuracy measurement of binary descriptors in mobile augmented reality	Floating point descriptor is not suitable for real-time application because of the operating speed and it does not satisfy real-time constraints	An efficient accuracy measurement using state of art binary descriptors thus, BRIEF, ORB, BRISK, and FREAK were used on the Mikolajczyk dataset and ALOI dataset.	The obtained result in this paper shows that FREAK is the most appropriate descriptor for the MAR application.	Only Mobile AR applications are considered
6	(Mohammed *et al.*, 2021)	Image Authentication Based on Watermarking Approach: Review	Transmission of the digital image through insecure media such as the internet.	A Survey approach is adopted by the researcher on techniques used in solving insecurity	the researchers finally concluded that the combination of the techniques will improve robustness, imperceptibility, and capacity	The research work is only limited to improving security using watermarking techniques

7	(Thaiyalnayaki & Devi, 2018)	Protection of Data in Cloud Computing using Image Processing Watermarking Technique	Ensuring digital image integrity has become a serious challenge in recent years	A robust reversible RSA, DCT, SVD, and DWT techniques were implemented on the cloud	Secured cloud service for securing client data	Securing cloud data using watermarking techniques is consider
8	(Sowmya *et al*., 2021)	Protection of data using watermarking techniques	Safety and limited capacity of watermarking embedding	A nested watermarking approach is present along with an A5/1 encryption algorithm	the approach increases watermarking embedding capacity and increases data safety	The researcher focuses only on capacity and safety
9	(Fita & Endebu, 2019)	Watermarking Colored Digital Image Using Singular Value Decomposition for Data protection	Due to the high integration of computers with the internet, the distribution of data becomes faster and easier, so duplication of multimedia content requires less effort	Singular Value Decomposition (SVD) was adopted for secure multimedia content	A robust watermarking scheme against geometric attacks	A single approach is only used in the research work. Another approach is not considered
10	(Soualmi *et al.*, 2020)	A novel blind Watermarking approach for medical image authentication using MinEigen Value Features	Based on the special attribute of medical image, the developing of watermarking techniques for the feature becomes highly necessary	The use of the Min Eigen Value feature, chaotic sequence, and Quantization Index Modulation (QIM)	The outcome of the research demonstrates high robustness to all DICOM JPEG compression attacks, while the imperceptibility is highly kept	The researcher focuses on the medical image only

11	(Srivastava *et al.*, 2021)	Image Watermarking Approach Using a Hybrid Domain Based on Performance Parameter Analysis	The traditional Frequency transform domain techniques are costly and complex. This degrades the quality of the image based on lesser embedding bit	DCT and DWT hybridized approach is considered	Improve performance based on time, robustness, and imperceptibility	Frequency domain approaches are only considered in the paperwork.
12	(Alshoura *et al.*, 2021)	Hybrid SVD-Based Image Watermarking Scheme: A Review	Many existing hybrid SVD image watermarking scheme is found to be insecure. And unavailability of in-depth review on that particular domain	An efficient comparison to identify security challenges in hybridize SVD scheme	Essential information is provided on how to develop a more robust watermarking scheme in the future	Comprehensive research on only the Hybrid SVD domain.
13	(Ray & Roy, 2020)	Recent trends in image watermarking techniques for copyright protection	malicious use and privacy have become the general medium for information transmission	the researcher designed different image watermarking steps to protect the copyright of the digital subject	the experimental results showed that the proposed scheme can resist different types of image-processing attacks	The research work only focuses on copyright protection
14	(Selvakumari & Jeyaraj, 2018),	Using Visible and Invisible Watermarking Algorithms for Indexing Medical Images	Though perfect methodologies for indexing the medical images would provide quick retrieval performance	In this paper the researcher carries out image watermarking steps for indexing medical images, also an experiment is carried out on embedding and extraction of both visible and invisible watermarking algorithms	for embedding purposes, LBP shows better performance in the case of extraction purposes, and IWT shows better performance where LBP shows the least.	The research work is limited only to medical image

15	Amiri, (2022)	Non-blind Arnold Scrambled Hybrid Digital Image Watermarking Scheme based on Differential Evolution and DnCNN Non-blind Arnold Scrambled Hybrid Digital Image Watermarking Scheme based on Differential Evolution and DnCNN	The author identifies that many algorithms that make use of SVD, always have false positive problem	The researcher makes use of three transforms with a differential evolutional algorithm	An enhance robust SVD algorithm schemes	The researcher tends to only consider enhancing SVD techniques,
16	Meg, (2022)	The architecture of a fake news detection system combining digital watermarking, signal processing, and machine learning	Much fake news and information is been circulated which is becoming a threat to each people and different sectors	the main goal of this research work is to create a tool that makes use of digital watermarking techniques, machine learning, and digital processing for detecting fake news	A fake news detector system	The designed system is only focused on detecting fake news.

17	(Sowmya *et al.*, 2021)	Protection of data using watermarking techniques	Safety and limited capacity of watermarking embedding	A nested watermarking approach is present along with an A5/1 encryption algorithm	the approach increases watermarking embedding capacity and increases data safety	The researcher focuses only on capacity and safety
18	Begum & Uddin, (2020)	Analysis of Digital image watermarking techniques through hybrid methods	Faced with the computational complexity of watermarking embedding and extraction. The existing singular digital image watermarking techniques cannot obtain all the design goals, such as imperceptibility, robustness, security, and capacity simultaneously with perfection.	DCT is used to ensure the visual quality of the host image, and a random binary matrix is used to improve the security of the digital image	Multiple image watermarking technique is designed that embeds several watermarks into the same host image for conveying multiple information.	The future work can be extended by simulating the results under several single and combined attacks for better robustness, imperceptibility, and security. Also, the performance of the proposed method will be compared with the existing method and expanded for other multimedia elements.

19	(Li *et al.*, 2021)	A double-encrypted watermarking algorithm based on cosine transform and fractional Fourier transform in the invariant wavelet domain	The existing watermarking algorithms invariant wavelet domain are weak at resisting geo-metric attacks and have small embedding capacities	Fractional Fourier transforms (FRFT) and discrete cosine transform (DCT) in the invariant wavelet domain is proposed.	The simulation results and comparative experiments show that the proposed algorithm exhibits high robustness under the premise of satisfying security, reliability, and invisibility, especially for geometric attacks such as rotation, cropping, and translation.	The robust watermarking algorithm Presented in this paper only performs the single function of protecting copyrights for the digital image. Their algorithm is designed for gray host images and watermarks, and it is not suitable for color images. The average PSNR is 33.518 dB which can be improved upon future study proposed the use of new and more effective measurement matrix for compressive sensing, it is possible for us to come up with a new binary feature descriptor which can be use like BRIEF into pattern recognition
20	Zhang *et al.*, 2015	Design of Binary Robust Independent Elementary Features (BRIEF) through Compressive Sensing View	Is a quite simple local feature descriptor. BRIEF address the challenges of pattern recognition and movement tracking in computer vision field.	Used the method of compressive sensing theory in proposing the reason why it works and guiding the parameter determination of BRIEF.	BRIEF is analyzed from the view of Compressive Sensing. which proves that BRIEF is the Binarization of Compressive Sensing Sampling. From the Compressive Sensing point of view, it is quite straight forward to understand why	

					BRIEF's performance is so good.	and movement tracking tasks.
21	Calonder *et al.*, 2011	BRIEF: Computing a local binary descriptor very fast	Face recognition, fast to compute feature matching and very limited computational power challenges faced by SURF, SITF are address in this paper by BRIEF which yields comparable recognition accuracy in comparison to other feature point descriptors that involves moving from the Euclidean to the Hamming distance for matching purposes	This paper used two approaches the Census transform and local binary pattern (LBP), that was designed to produce a robust descriptor robust. This descriptor is non-parametric and local to some neighbourhood around a given pixel.	BRIEF descriptor of relatively small number of intensity difference tests to represent an image patch as a binary string. The construction and matching of BRIEF descriptor are much faster than other state-of-the-art such as SURF, SIFT, BRISK and FAST it also tends to yield higher recognition rates, as long as invariance to large in-plane rotations is not a requirement.	Future work will aim at developing data structures that allow for sub-linear time look-up of BRIEF descriptors.

2.19.1 Summary of the Related Works

It was observed from the review work of literatures of Researchers; Mohammed *et al* (2021), and Begum & Uddin, (2020), did not provide enough metrics to be able to evaluate the robustness, imperceptibility, security, and efficiency of the techniques. Li *et al.*, 2021, presented a research work on Fractional Fourier transforms (FRFT) and discrete cosine transform (DCT) in the invariant wavelet domain. The robust watermarking algorithm presented only performs the single function of protecting copyrights for the digital image. The algorithm is designed for gray host images and watermarks and obtained an average PSNR value of 33.518 dB which can be improved upon (Li *et al.*, 2021). However, from the reviewed literatures none of them has hybridized BRIEF–SVD Techniques to a achieve a better result. Hence, this study proposed a hybrid BRIEF-SVD and four other metrics such as PSNR, SNR, MSE, and MAE, in order to give a more robust, imperceptible, secure, and efficient evaluation of the techniques.

CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 Introduction

This chapter opens the discussion on the techniques, approaches, or methods adopted in this study, and a tentative and comprehensive explanation of how data are generated where discussed. The hybridized techniques employed in this research work are equally presented. Lastly, all the evaluation metrics adopted to evaluate and validate the proposed hybridized techniques are also presented. Figure 3.1 represents the hybridization of the proposed methods.

Figure 3.1: The Proposed Hybrid Watermarking Approach

Figure 3.1 encapsulates the two proposed methods, SVD and BRIEF in subsections 3.1.1 and 3.1.2.

3.1.1 Singular Value Decomposition (SVD)

Image watermarking schemes based on singular value decomposition (SVD) is a powerful technique that is used for image processing and have become popular due to its high level of security and robustness.

The mathematical equation for singular value decomposition X is as follows:

$$\square = \square\square\square^{\square} \quad (3.1)$$

Where U is an $m \times n$ matrix, S is an $n \times n$ diagonal matrix, and V^T is also an $n \times n$ matrix. The columns of U are called the *left singular vectors*, $\{U_K\}$, and form an orthonormal basis for the assay expression profiles so that $U_i \text{ ‘ } U_j = 1$ for $i = j$, and $= 0$ and $U_i \text{ ‘ } U_j = 0$

otherwise. The rows of V^T contain the elements of the *right singular vectors, {V_k},* and form an orthonormal basis for the gene transcriptional responses. The elements of *S* are only nonzero on the diagonal and are called singular values (Fita & Endebu, 2019).

Different Versions of SVD are:

FULL SVD:

$$X_{n\times d} = U_{n\times n}\, \Sigma_{n\times d}\, V^T_{d\times d}.$$

COMPACT SVD:

Suppose rank(X) = r. Define

$U_r = [U_1 \ldots U_r] \in R^{n\times r}$

$V_r = [V_1 \ldots V_r] \in R^{d\times r}$

$\Sigma_r = \text{diag}(\sigma_1 \ldots \sigma_r) \in R^{r\times r}$

Furthermore, the process of Singular Value Decomposition is further discussed in the research work. The process involves the breaking down of a singular matric A into a sub-matric of A = □ ∑ □^{T}. This splitting computation enables the retaining of important

singular values which require and at the same time dropping the values which are not necessary for retaining or maintaining the image quality. The singular values of matrix A with (m x n) dimension are the square roots of the eigenvalues of the (n x n) A^T matrix A, which are organized in magnitude and decreasing order.

3.1.2 Binary Robust Independent Elementary Features (BRIEF)

Based on the fact that these technologies have to handle more data or are required to run on a mobile device with limited computational resources, the growing need for local description (BRIEF) that are fast to compute, match, and memory efficient is required. In term of speed and recognition rate BRIEF outperform other fast descriptors such as SURF, K-KAZE, FAST, and SIFT, the intensity test □ of a given smoothed image patch

The mathematical equation for binary robust independent elementary features (BRIEF) is as follows:

□ is defined as follows:

$$\square(\square;\square,\square) = \{ \begin{matrix} 1 & \square\square\ \square(\square) < \\ 0 & \square\square h\square\square\square\square\square \end{matrix} \quad (3.2)$$

Where □(□) represent the intensity of the pixel within the smoothed patch □ at point ***x.*** Here the outputs of the binary test are concatenated into a vector of n bits that is referred to as the descriptor (Zhang *et al.,* 2015) This vector of n bit string can be defined as:

$$\square_{\square}(\square) = \sum_{1\le\square\le\square} 2^{\square-1}\ \square(\square;\square_{\square},\square_{\square}) \quad (3.3)$$

3.2 The Proposed Conceptual Framework

This section presents the conceptual framework of this research study, along with their respective steps to actualize the objectives of the study. Similarly, the proposed approaches to the respective steps are shown in Figure 3.2.

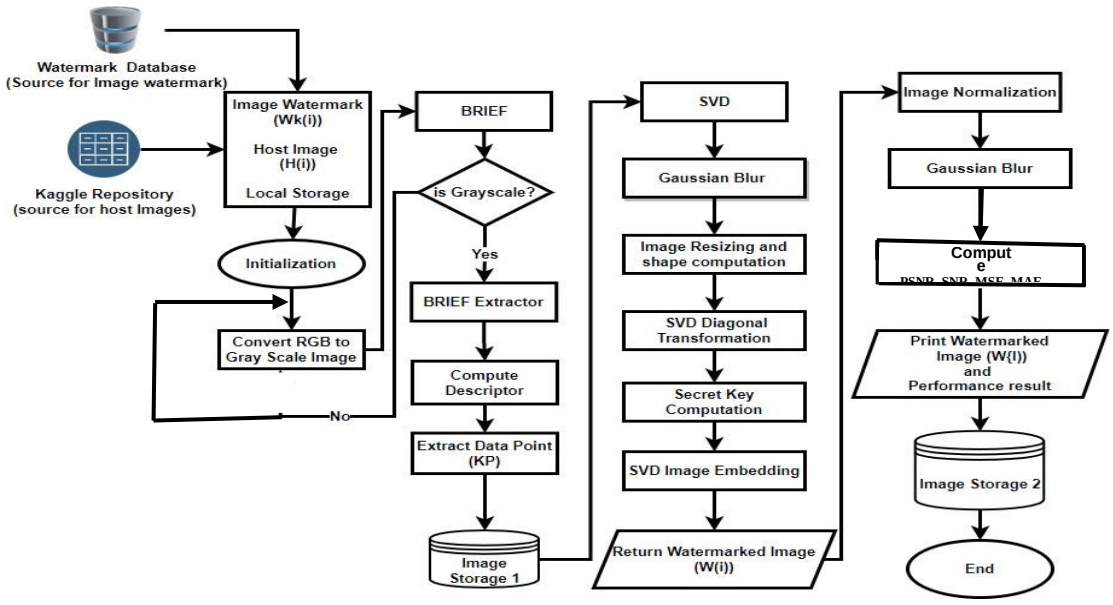


Figure 3.2: Conceptual Framework for the Proposed Hybrid Watermarking Scheme

The four main layers towards achieving the conceptual framework of the proposed hybrid watermarking scheme (Figure 3.2) are explained as follows:

3.2.1 Data Collection Layer

Step 1: The proposed conceptual framework of (Figure 3.2) begins with the data collection step, in which the image samples along with their properties such as dimension, height, width, horizontal resolution, vertical resolution, and bit depth have been collected from Kaggle dataset repository.

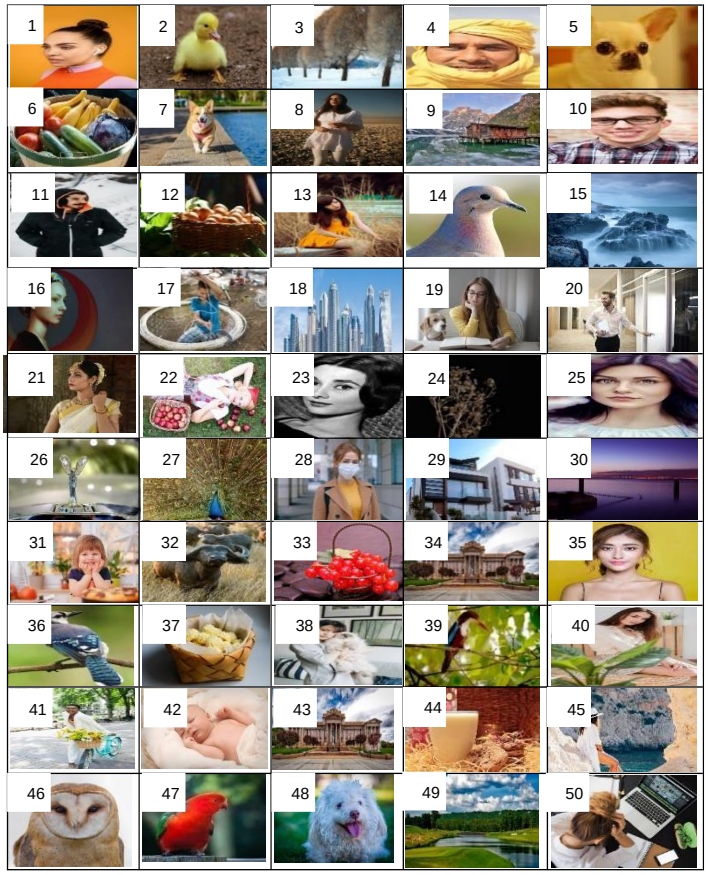


Figure 3.3 Complete 50 Host Image datasets from the Kaggle repository

Step 2: The host image (Hi), is the original image collected from the Kaggle repository while the watermark image (wki) is a small image that will be embedded in to the host image collected from Github.com, where some group of image watermark are being stored. The two images are stored in the local storage for easy accessibility and use.

Step 3: The initialization step prepares both the host image and the watermark image and load into the next step for conversion.

Step 4: Conversion of RGB image to a grayscale image, if the inputted host image is a grayscale image or an RGB image, depending on the choice of the image. In this study, a grayscale image was chosen as the choice of the image used. if the inputted host image (H(i)) is an RGB-based image, it is required to be converted to a grayscale image before feeding it into the brief algorithm.

3.2.2 BRIEF Layer

Step 5: The brief algorithm function is invoked for execution, the function checks if the image is an RGB or a grayscale. If the image is an RGB it will return to step 4 for pre-processing, otherwise continue with brief extraction.

Step 6: BRIEF is an image descriptor algorithm, that described images and serve as a numerical fingerprint which can be used to distinguish one feature from another. Before the BRIEF can performs any function, it inputs the BRIEF extractor to extract certain features from the image such as points that are located on the image. The BRIEF uses the values collected from the extraction process to compute the data point (KP) that is the new key point for the images. The data point (KP) is an intersection of two or more edge segments or point at which the direction of the objects border rapidly changes, Data point or the interest point preserves the quality of an image. The internal process that are inherent in the BRIEF algorithm are the extraction of data key points, compute descriptors and brief extractor.

Step 7: Once the data point has been identified and extracted, the newly processed image is saved into image storage one for the next step of processing.

3.2.3 SVD Embedding Layer

Step 8: This step involves image embedding and encoding using a singular value decomposition algorithm, it then applies gaussian blur to smoothen and enhanced the quality of the image before image resizing and formatting is done. During the process of resizing the image, shape computation is carried out to prepare the image for SVD diagonal transformation.

Step 9: For SVD diagonal transformation the images are being converted into matrix form as every image is seen in a form of matrix (0,1) each pixel contains number from 0-255 where the secret key is computed.

Step 10: The secret key generation algorithm, generates and embedded the secret key that contains numbers and characters, where the watermark image is also embedded into the processed image using the SVD embedding technique, and the watermarked image moves to the next step for image normalization.

3.2.4 Image Normalization Layer

Step 11: The image from SVD embedding technique is moved to image normalization in rough matrix form and need to be converted to the original image. Image normalization is the process of converting image that is in a form of matrix back to original image, where the gaussian blur technique is implemented to denoise the image.

Step 12: The next step involves measuring the performance of the entire process of image watermarking, this is done by computing the Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Means Absolute Error (MSE), and Means Square Error (MAE). After the computation process of the performance metrics, the watermarked image is stored on image storage two, and the process of image watermarking is completed.

3.3 Algorithmic Representation of the Proposed Hybrid Methods

The algorithmic representation of the hybridization of two methods is succinctly explained to show the procedures towards achieving the implementation of an enhanced watermarking scheme.

Algorithm 3.1: An enhanced Hybrid BRIEF_SVD watermarking Techniques

---

Parameters: The input image for the Host is defined by (Hi), the watermark is denoted by (Wki), The BRIEF extractor is denoted by (BEi), The watermarked Image is denoted by (Wi), The secret Key is (K) and Data point (KP).

Input: (Hi), (Wki)
Output: (Wi)
Procedure:

1. Watermarked Image (Wi) = BRIEF (bi) + SVD (si)
2. Input Image1, Image2 from local Storage
3. Initialize Host Image (Hi) as Image1, Watermark (Wki) as Image2:
4. Convert (Hi) and (Wki) to grayscale
5. **Call BRIEF ():**

If ((Wki) AND (Hi)! = Grayscale): //**checks if image is in grayscale**
Return to step 4
Else:
Continue:
Initialize BRIEF Extractor BEi
Compute Descriptor (Des) and Determine DataPoint (KP)

Return Saveimage(img).

6. **Call SVD():**

CoverImage = Read SavedImage(img)//**reads processed image from step5**
CoverImage = GaussianBlur (CoverImage) //**applies Gaussian smoothing**
CoverImage = Resize(CoverImage) // **resize the image**
Compute Shape of Resized Image //**compute shape for embedding**

```
[m,n]=np.shape(coverImage)
CoverImage=np.double(coverImage)
watermarkImage = cv2.resize(watermarkImage,(256,256))
```

// **secretkey Generation**
K = generateSecret()

//**modifying diagonal component SVD Image Transformation**

```
for i in range(0,x):
        for j in range(0,y):
        Wcvr[i,j]=(Wcvr[i,j]+0.01*watermarkImage[i,j])/255
```

//**Watermarked Image Embedding procedure**

```
S=np.zeros((512,512),np.uint8)
```

```
S[:m,:n]=np.diag(w)
S=np.double(S)
wimg=np.matmul(ucvr,np.matmul(S,vtcvr))
wimg=np.double(wimg)
wimg*=255
watermarkedImage = np.zeros(wimg.shape,np.double)
```

7. Normalize WaterMaked Image (Wi)

```
normalized=cv2.normalize(wimg,watermarkedImage,1.0,0.0,cv2.NORM_MINMAX)
```

8. Apply Gaussian Blur
9. **Save** the WaterMarkedImage(Wi).
10. Compute PNSR, SNR, MSE and MAE //performance metrics computation
11. **Return** (Wi)
12. **END**

From an enhanced algorithm 3.1, parameters, input, output and functions, are defined.

Lines 1 to 2 shows the general formula for the hybridization of two key algorithms (bi), (si), and the process of inputting image 1 and image 2 into the local storage.

Lines 3 to 4 initialize and assign the inputted images to their respective variables (hi) and (wki), resizing and reshaping of the two images are done at the initialization step. image (hi) and (wki) are converted to a grayscale image, then the algorithm will proceed to call on the brief function.

Line 5 Consequently, the brief function checks if the (wki) and (hi) are grayscale images, if the condition is satisfied it will continue to compute the brief descriptor and draw datapoint on the image. Else the image return to line 4.

Line 6 reads the processed image from line 5 and calls the SVD function for embedding, applying Gaussian smoothing and resizing the image. The SVD generates a secret key and reshapes the image, then modifies the diagonal matrix for SVD transformation and embeds the watermark.

Lines 7 to 9: After the embedding occurs, the normalization and formatting of watermarked image (wi) are also done by SVD as every image is seeing in a form of a

matrix, there is a need for it to be presented as an image before applying Gaussian blur to reduce data loss, noise and save the watermarked image.

Finally, the performance metrics such as Peak Signal to Noise Ratio, Signal to Noise Ratio, Means Square Error, And Means Absolute Error was computed into the algorithm. Then output the watermarked image and end the process which is indicated from line 10 to 12.

3.4 Requirements of the Watermarked Scheme

The development of the proposed watermarked scheme consists of two important requirements namely; the software and hardware.

Software: Python programming language, Anaconda Integrated Development Environment (IDE), Spyder Text Editor, open CV Library, MatPlotLib, Numpy Library and Image Resizer tool software were used for the implementation of the watermarked scheme.

Hardware:

The hardware components used for the implementation are the CPU processor of 2.5 GHZ, Laptop with the capacity of 4 GB RAM, 150 GB Hard Disk and 3.0 USB space.

3.5 Performance Evaluation Metrics

Performance evaluation metrics are regarded as an important phase in research work, in which standard goals are measured to compare experimental results with the existing works. In computing-related research works, evaluation is a measure for assessing and validating the degree of achievement of a technique.

3.5.1 Peak Signal-to-Noise Ratio (PSNR)

Peak-Signal-to-Noise Ratio PSNR is commonly used to examine the quality of the image or frame, which is calculated as the ratio between the maximum possible power of the original image and the power of the watermarked image. The main advantage of PSNR is that it improves data confidentiality and robustness.

The mathematical representation of PSNR is as follows:

$$PSNR = 20\log_{10}\left(\frac{\square\square\square_{\square}}{\sqrt{\square\square\square}}\right) \quad (3.4)$$

Where:

$\square\square\square_{\square}$ is the maximum signal value that exists in its original form "know to be good" image (Gupta & Ahmad, 2017).

3.5.2 Mean Square Error (MSE)

Mean square error is inversely related to the peak signal-to-noise ratio and is determined between the original frame and watermarked frame to verify distortion after the watermark embedding process (Arora, 2018).

The mathematical representation of MSE is as follows:

$$\square\square\square = \frac{1}{\square\square} \sum_{0}^{\square-1} \sum_{0}^{\square-1} ||\square(\square,\square) - \square(\square,\square)||^2 \quad (3.5)$$

Where:

f: represent the matrix data of our original image.

g: represents the matrix data of our degraded image.

m: represent the number of rows of pixels of the images and i represent the index of that row.

n: represents the number of columns of pixels of the image and j represents the index of that column.

3.5.3 Signal-to-Noise Ratio (SNR)

SNR describes the total noise present in the output edge detected in an image, in comparison to the noise in the original signal level. SNR is a quality metric and presents a rough calculation of the possibility of false switching, it serves as a means to compare the relative performance of the different implementations (Menendez-Ortiz *et al.*, 2019).

The mathematical representation of SNR is as follows:

$$SNR = 10\log\left(\frac{\sum_{n=1}^{N} f(n)^2}{\sum_{n=1}^{N} [f(n) - \hat{f}(n)]^2}\right) \quad (3.6)$$

Where:

$f(n)$ is a signal containing noise

$\hat{f}(n)$ is a denoise signal

N is the length of the signal.

The smaller the MSE, the greater the SNR, and the better the denoising effect.

3.5.4 Mean Absolute Error (MAE)

Mean absolute error (MAE) is a measure of errors between paired observations expressing the same phenomenon. The lower the mean absolute error and closeness to zero the better the results (Series & Science, 2018).

$$MAE = \frac{\sum_{i=1}^{n} |y_i - x_i|}{n} \quad (3.7)$$

Where:

MAE denotes Mean Absolute Error

$\mathbf{y_i}$ represents prediction

$\mathbf{x_i}$ represents the true value

n denotes the total number of data points

CHAPTER FOUR

4.0 RESULTS AND DISCUSSION

4.1 Experimental Results

The experimental results obtained for both the existing and the proposed techniques are presented in this section. The experiments were carried out using three images (pixels) with the dimensions 512x512 each. The performance of the proposed techniques was measured and compared with the existing techniques using metrics that include Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Mean Square Error (MSE), and Means Absolute Error (MAE).

4.2 Singular Value Decomposition (SVD)

Tables 4.1a and 4.1b present the experimental findings from the application of the SVD watermarking technique to the images. In order to evaluate the effectiveness of the technique, metrics; SNR, PSNR, MSE, and MAE were used.

Table 4.1a: Experimental Results for Singular Value Decomposition (SVD)

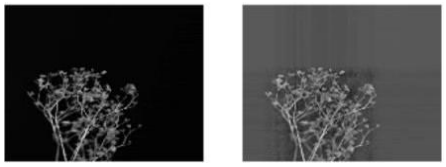
SN	Image	Original Image Vs. Watermarked Image	Result Obtained
1.	Flower Image		PSNR= 26.73 MSE = 29.98 SNR = -6.26 MAE = 44.2
2.	Human Image		PSNR = 35.55 MSE = 9.66 SNR = 12.78 MAE = 3.098
3.	Animal Image		PSNR = 30.56 MSE = 9.20 SNR = 15.19 MAE = 4.41

Table 4.1b Results on Singular Value Decomposition (SVD)

IMAGES	PNSR	SNR	MSE	MAE
Flower Image	26.73	6.26	29.98	44.20
Human Image	35.55	12.78	9.66	3.09
Animal Image	30.56	15.19	9.20	4.41
Average	30.95	7.24	19.82	17.24

4.3 Discrete Wavelet Transform (DWT)

Tables 4.2a and 4.2b present the results of applying the DWT on three Images. The result shows the performance of the technique based on four metrics; SNR, PSNR, MSE, and MAE.

Table 4.2a: Experimental Results of Discrete Wavelet Transforms (DWT)

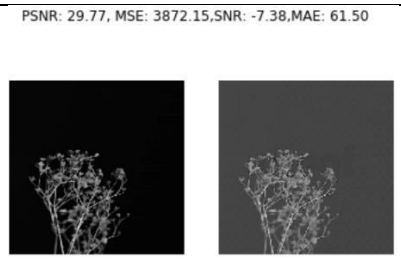
SN	Image	Original Image Vs. Watermarked Image	Result Obtained
1.	Flower Image		PSNR= 29.78 MSE = 38.02 SNR = 7.38 MAE = 61.50
2.	Human Image		PSNR = 27.72 MSE = 7.84 SNR = 3.81 MAE = 25.58
3.	Animal Image		PSNR = 28.12 MSE = 7.69 SNR = 5.91 MAE = 23.00

Table 4.2b: Results of Discrete Wavelet Transforms (DWT)

IMAGES	PNSR	SNR	MSE	MAE
Flower Image	29.78	7.38	38.02	61.50
Human Image	27.72	3.81	7.84	25.58
Animal Image	28.12	5.91	7.69	23.00
Average	28.54	5.70	17.85	36.69

4.4 Singular Value Decomposition – Discrete Wavelet Transform (SVD-DWT)

Tables 4.3a and 4.3b show the results of hybridized SVD-DWT on three Images (Flower, Human and Animal Image). The performance was evaluated using metrics; SNR, PSNR, MSE, and MAE.

Table 4.3a: Experimental Results for the Hybridization of SVD-DWT

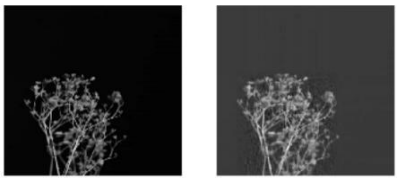
SN	Image	Original Image Vs. Watermarked Image	Result Obtained
1.	Flower Image		PSNR = 26.73 MSE = 29.98 SNR = -6.27 MAE = 54.21
2.	Human Image		PSNR = 27.40 MSE = 1.90 SNR = 9.76 MAE = 12.62
3.	Animal Image		PSNR = 28.01 MSE = 12.43 SNR = 3.89 MAE = 28.75

Table 4.3b: Results on Hybridization of SVD-DWT

IMAGES	PNSR	SNR	MSE	MAE
Flower Image	26.73	6.27	29.98	54.21
Human Image	27.40	9.76	1.90	12.62
Animal Image	28.01	3.89	12.40	28.75
Average	27.38	2.46	14.76	31.86

4.5 Binary Robust Independent Elementary Features (BRIEF)

Tables 4.4a and 4.4b show the results of applying the BRIEF on three Images. The performance of the technique was evaluated based on SNR, PSNR, MSE, and MAE.

Table 4.4a: Experimental Results of BRIEF

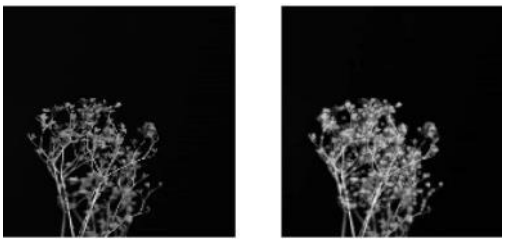
SN	Image	Original Image Vs. Watermarked Image	Result Obtained
1.	Flower Image		PSNR =34.40 MSE = 430.85 SNR = 2.16 MAE= 8.48
2.	Human Image		PSNR = 30.41 MSE = 198.53 SNR = 9.78 MAE = 9.50
3.	Animal Image		PSNR = 30.19 MSE =230.16 SNR = 11.22 MAE=10.35

Table 4.4b: Results on Binary Robust Independent Elementary Features (BRIEF)

IMAGES	PNSR	SNR	MSE	MAE
Flower Image	34.40	5.20	4.30	8.47
Human Image	32.40	9.78	1.98	9.50
Animal Image	30.19	11.30	2.30	8.34
Average	32.33	8.76	2.86	8.77

4.6 Singular Value Decomposition - Binary Robust Independent Elementary Features (SVD-BRIEF)

Tables 4.5a and 4.5b present the results of applying the hybridized BRIEF-SVD on three Images. The results show the performance of the techniques using PSNR, SNR, MSE, and MAE.

Table 4.5a Experimental Results for Hybridization of BRIEF-SVD

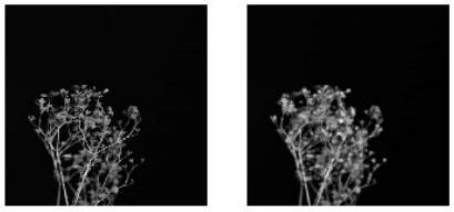
SN	Image	Original Image Vs. Watermarked Image	Result Obtained
1.	Flower Image		PSNR = 34.45 MSE = 2.80 SNR = 10.20 MAE = 6.88
2.	Human Image		PSNR = 33.64 MSE = 1.90 SNR = 9.90 MAE = 8.90
3.	Animal Image		PSNR = 34.78 MSE = 2.30 SNR = 14.22 MAE = 5.34

Table 4.5b: Results on Hybridization of BRIEF-SVD

IMAGES	PNSR	SNR	MSE	MAE
Flower Image	34.45	10.20	4.20	6.40
Human Image	33.64	9.90	1.90	8.90
Animal Image	34.78	14.22	2.30	5.34
Average	34.29	11.44	2.80	6.88

4.7 Summary of Results.

Table 4.6 presents the overall results of all the techniques and metrics used to evaluate the performance of each technique.

Table 4.6: Final Results of the Performance Metrics

Techniques	PSNR	SNR	MSE	MAE
DWT	28.54	5.70	17.85	36.69
SVD	30.95	7.24	19.82	17.24
BRIEF	32.33	8.76	2.86	8.77
SVD - DWT	27.38	2.46	14.76	31.86
BRIEF-SVD	34.29	11.44	2.80	6.88

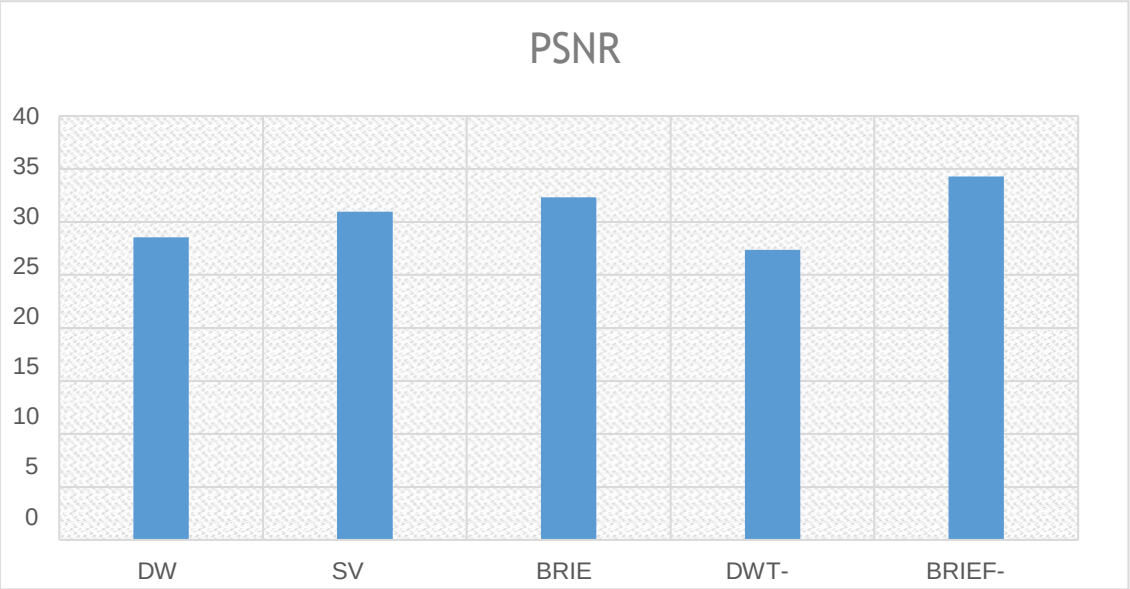


Figure 4.1: Bar Chart of Peak Signal to Noise ratio (PSNR)

Figure 4.1, DWT, SVD, BRIEF, hybridization of DWT-SVD, and hybridization of BRIEF-SVD have been tested by PSNR. The higher the value of PSNR the better the quality of the watermarked image. Therefore, BRIEF-SVD has the highest value of PSNR which indicates good performance.

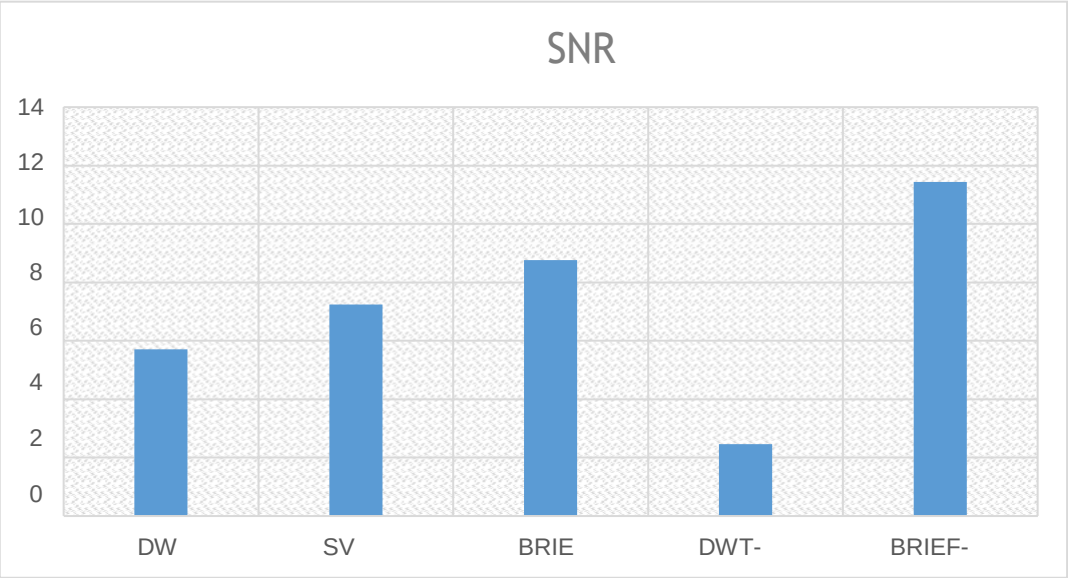


Figure 4.2: Bar Chart Signal to Noise ratio (SNR)

Figure 4.2, the higher the values of SNR indicate that the image quality is stronger in relation to the noise levels. BRIEF-SVD and BRIEF Performed better than other techniques. DWT, SVD, and DWT-SVD performed less than average.

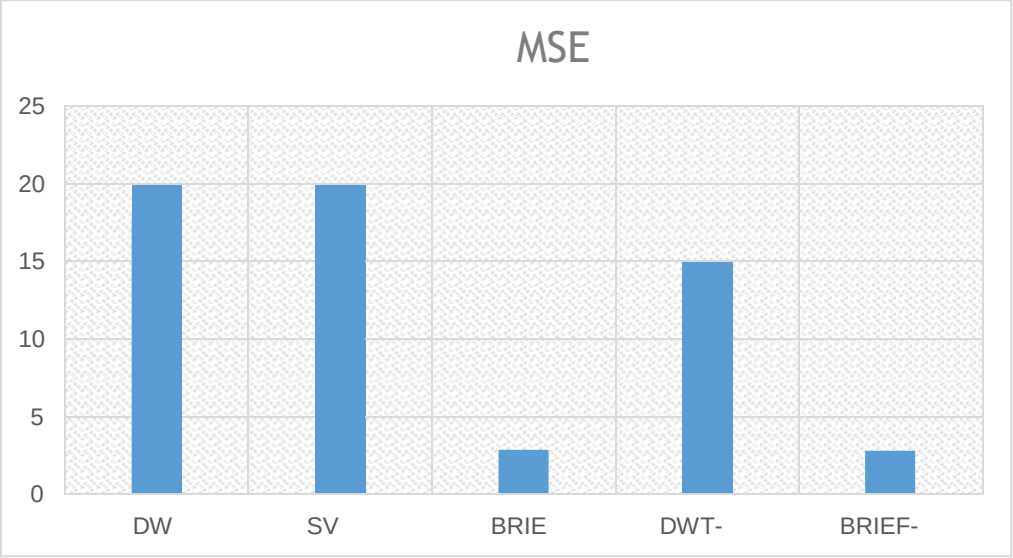


Figure 4.3 Bar Chart showing the Mean Square Error (MSE) of all Techniques

Figure 4.3 shows the Means Square Error obtained from each technique and the lower the MSE, the better the image quality. BRIEF-SVD has the best performance in comparison to BRIEF, DWT, SVD, and DWT-SVD.

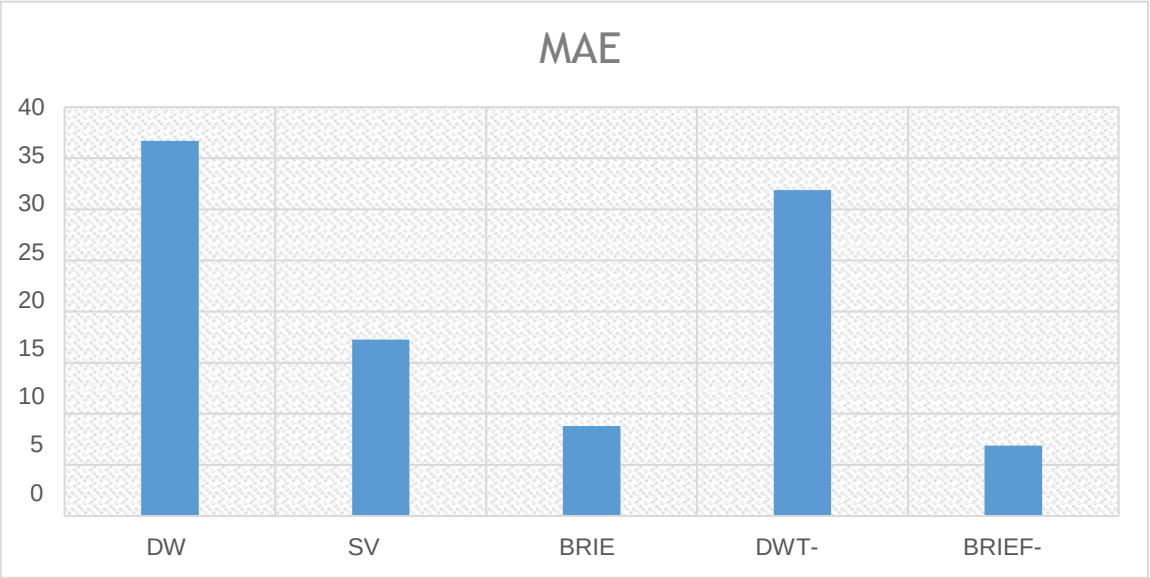


Figure 4.4 Bar Chart showing Mean Absolute Error (MAE)

Figure 4.4 shows the bar chart of mean absolute error. MAE can range from 0 to ∞. They are negatively-oriented scores: Lower values are better. Hence, from the graph (figure 4.4), BRIEF-SVD has the best performance compared to BRIEF, DWT, SVD, and DWT-SVD.

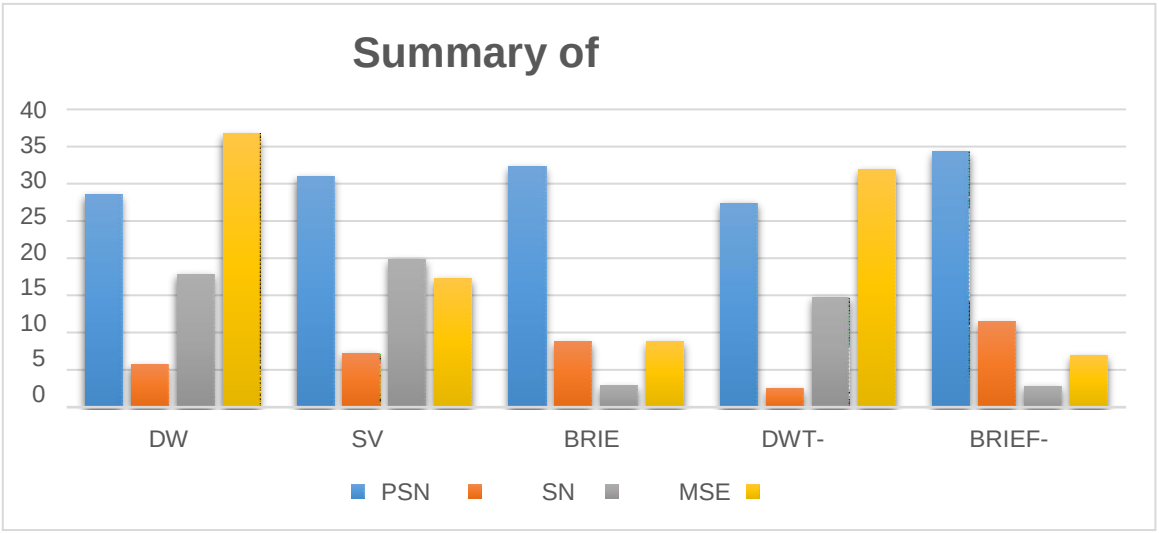


Figure 4.5: A Chart Comparing the Performance of Five Different Techniques

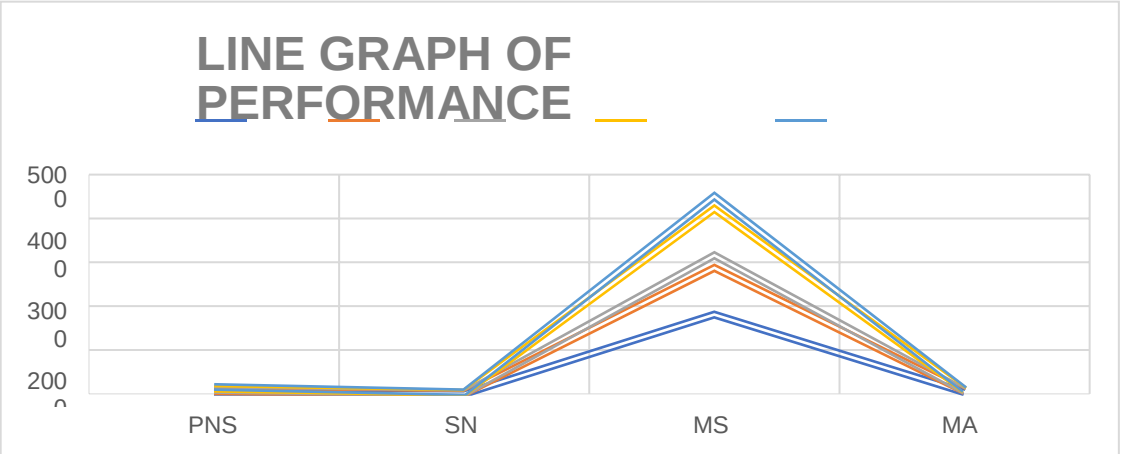


Figure 4.6 Shows the Line Graph of Five Different Techniques

Figure 4.6 represents a line graph that further shows a newer dimension in order to understand the results obtained using performance metrics such as PSNR, SNR, MSE, MAE. Again, BRIEF-SVD outperformed BRIEF, SVD, DWT, and SVD-DWT.

4.8 Result Discussion and Analysis

The most vital reasons for adopting the hybridization of watermarking techniques and feature descriptors such as Binary Robust Independent Elementary Features (BRIEF), Singular Value Decomposition (SVD), and Discrete Wavelet Transform (DWT) in this scheme is to analysed results and enhance the effective performance of individual techniques (algorithms) used in the scheme and also to justify that hybridization of BRIEF-SVD had proven to be more efficient as shown by the results obtained.

Metrics such as PSNR, SNR, MSE, and MAE are used to assess the performance of these techniques. In table 4.5b, the proposed method BRIEF-SVD yielded the best results, with an average PSNR value of 34.29dB, SNR value of 11.44dB, MSE value of 2.8, and MAE of 6.88, while BRIEF yielded a PSNR value of 32.33db, SNR value of 8.76dB, MSE value of 2.86, and MAE of 8.77.

According to the results obtained from table 4.3b the hybridization of SVD-DWT has a PSNR value of 27.38dB, SNR value of 2.46033dB, MSE of 14.76, and MAE of 31.86, in table 4.2b it is also observed that DWT takes the PSNR value of 28.54dB, SNR of 5.7dB, MSE value of 17.85 and the MAE value of 36.6933.

In table 4.1 SVD has the average PSNR value of 30.9466dB, SNR value of 7.236dB, MSE of 19.82, and MAE of 17.2373 respectively.

Considering the results of the proposed BRIEF-SVD, it achieved the highest PSNR, SNR, and lowest MSE, MAE values, where the higher the PSNR and SNR values, the better the quality of the watermarked image, and the lower the values of MSE and MAE, the better the result. This shows that the hybridization of the BRIEF-SVD watermarking scheme is more secure and robust, which is in line with the objectives of this study. The result obtained from table 4.6 shows the summary of all the techniques and metrics. The results also shows that the BRIEF-SVD outperformed all the remaining techniques.

It is also observed in figures 4.1 and 4.2 that PSNR and SNR results obtained from table 4.6 BRIEF-SVD has outperformed all the algorithms in terms of PSNR, SNR, MSE, and MAE values while those in table 4.6, figures 4.3 and 4.4 were analyzed in terms of lower error rate where DWT has the value of 17.85 and 36.69, SVD 19.82 and 17.23, DWT-SVD 14.76 and 31.86, BRIEF 2.86 and 8.77.

Furthermore, the BRIEF-SVD gave the MSE and MAE values of 2.8 and 6.88. This outstanding performance by BRIEF-SVD with minimum error of 2.8 and 6.88 in table 4.7 indicates good image quality, image protection, and robustness against various types of image processing attacks such as high levels of piracy, theft, and illegal distribution of multimedia materials.

Figure 4.5 and 4.6 presents an overview of the results from figures 4.2, 4.3, and 4.4, (PSNR), (SNR), measured in Decibel (dB), is said to be good if the result is above zero and tends towards 40dB. From the graph, BRIEF-SVD and BRIEF have better results of PSNR of 34.29dB, 32.33dB, and SNR of 11.44dB, 8.746dB respectively, making BRIEF-SVD the best-performing technique in terms of noise ratio. Not only do BRIEF-SVD performs efficiently in terms of PSNR and SNR but it also performs incredibly well in terms of MSE and MAE.

Table 4.7 shows a detailed comparison of the previous research works and performance evaluation of proposed BRIEF-SVD technique.

Table 4.7: Result Comparison for the Evaluation Performance of the Algorithms

Existing works	Techniques	PSNR	SNR	MSE	MAE
Begum & Uddin, (2020)	DCT	30 dB	-	-	-
Mohammed *et al., (*2021)	DCT, DWT, SVD	-	-	-	-
Li *et al.,* (2021)	FRFT, DCT	33.518 dB	-	-	-
Proposed Technique	**BRIEF-SVD**	**34.29 dB**	**11.44 dB**	**2.8**	**6.88**

It can be deduced from Table 4.7 that the performance of the proposed hybrid watermarking technique BRIEF-SVD gave a better result with four metrics when compared with those of the previous techniques by Begum & Uddin, (2020), Mohammed *et al., (*2021) and Li et al., (2021) reviewed in the literature. This result indicates that the hybridization of BRIEF-SVD has outperformed the existing techniques.

4.9 Performance Validation

The performances of the watermarking technique are benchmarked alongside and matched with the performances of some previous works that use related works are; Begum & Uddin, (2020), Mohammed *et al.,* (2021) and Li *et al.,* (2021). The comparison is shown in Table 4.7.

CHAPTER FIVE

5.0 CONCLUSION AND RECOMMENDATION

5.1 Conclusion

In conclusion, this study proposed and implemented BRIEF+SVD using gray-scale images while designing an efficient watermarking scheme, based on the result obtained BRIEF proves to be a good image descriptor. The hybrid methods BRIEF and SVD yield better results during the cause of the implementation. The evaluation results obtained indicated that the hybridization of BRIEF and SVD outperformed other existing techniques, having the PSNR value of 34.29dB, SNR of 11.44dB, MSE of 2.8 and MAE 6.88. With this remarkable performance of BRIEF+SVD, it is concluded as the best technique in the proposed watermarked scheme. The results of this study have shown that the previous performances have been improved upon which satisfied the objectives enlisted to pursue the goal of this research work.

Finally, to design an efficient watermarking (scheme), this research concludes that the hybridization of watermarking techniques and feature descriptors could be more efficient, imperceptible, secured, and robust. Because BRIEF-SVD performs excellently well, and so it is recommended as the best technique when designing an efficient watermarking scheme.

5.2 Recommendations

This study has effectively developed and presented a conceptual framework for a hybrid watermarked scheme that enhanced the security, imperceptibility, and robustness of the watermarked scheme. In this study, the proposed watermarking scheme gave a remarkable result by improving its security and robustness. However, future research study in the watermarking scheme is recommended in order to achieve a higher

superiority technique. In addition to future work, it is recommended that researchers should consider using error measuring algorithm to determine the effective performance of the watermarked scheme and may also increasing the number of images used in conducting the experiment.

5.3 Contributions to the knowledge

This research has made contributions to knowledge by:

i. Successfully developing a hybrid watermarking scheme for data protection in cloud computing, which is implemented by using a hybrid BRIEF-SVD algorithm that enhanced security alongside the security threats against multimedia contents.

REFERENCES

Abdalla, P. A., & Varol, A. (2019). Advantages to Disadvantages of Cloud Computing for Small-sized Business.*2019 7th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). *IEEE*. https://doi.org/10.1109/ ISDFS.2019. 8757549

Abdel-Basset, M., Mohamed, M., & Chang, V. (2018). NMCDA: A Framework for Evaluating Cloud Computing Services. *Future Generation Computer Systems*, 86, 12–29. https://doi.org/10.1016/j.future.2018.03.014

Agarwal, N., Singh, A. K., & Singh, P. K. (2019). Survey of Robust and Imperceptible Watermarking. *Springer, Multimedia Tools and Applications, Springer* 78(7), 8603–8633. https://doi.org/10.1007/s11042-018-7128-5

Agrawal, T. (2015). A Survey on Information Hiding Technique Digital Watermarking. 3(8), 68–74. *Proceedings of 29th IRF International Conference*, Pune, India, https://doi:10.18479/ijeedc/2015/v3i8/48358.

Ahmad, D. A., (2018). Cloud Computing-Positive Impacts and Challenges in Business Perspective. *Journal of Computer Science & Systems Biology*, 12(01), 15–18. https://doi.org/10.4172/jcsb.1000294

Alalawi, A., & Al-Omary, A. (2020). Cloud Computing Resources: Survey of Advantage, Disadvantages and Pricing. *2020 International Conference on Data Analytics for Business and Industry*: *(ICDABI)* (pp.1-6). *IEEE Expl*ore. https://doi:10.1109/icdabi51230.2020.9325645

Alam, T. (2020). Cloud Computing and its Role in the Information Technology. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, 1(2), 108-115. doi:10.2139/ssrn.3639063.

Alhenaki, L., Alwatban, A., Alamri, B., & Alarifi, N. (2019). A Survey on The Security of Cloud Computing. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-7). IEEE. https://doi: 10.1109/CAIS.2019.8769497

Ali, N. (2018). A Comparison between Cluster, Grid, and Cloud Computing. *International Journal of Computer Applications,* 179(32), 37–42. https://doi.org/10.5120/ijca2018916732

Alshoura, W. H., Zainol, Z., & Teh, J. E. S. E. N. (2021). Hybrid SVD-Based Image Watermarking Schemes: A Review. *IEEE, Access* (9). pp 32931–32968. https://doi.org/10.1109/ACCESS.2021.3060861.

Amiri, A. (2022). Non-blind Arnold Scrambled Hybrid Digital Image Watermarking Scheme Based on Differential Evolution and DnCNN, *Department of Computer Engineering, Shahid Rajaee Teacher Training University,* Tehran, Iran doi: https://doi.org/10.21203/rs.3.rs-1531091/v1

Anil, A., Shukla, V. K., & Mishra, V. P. (2020). Enhancing Data Security Using Digital Watermarking. *Proceedings of International Conference on Intelligent Engineering and Management (ICIEM), London, UK*, 364–369. https://doi.org/10.1109/ICIEM48762.2020.9160090.

Anitha, P., & Patil, M. M. (2016). A Survey on Watermarking Methods for Security of Cloud Data. *International Journal of Advance Research in Science and Engineering*. pp 556-564, ISBN: 978-81-932074-1-3

Arora, S. M. (2018). A DWT-SVD Based Robust Digital Watermarking for Digital Images. *International Conference on Computational Intelligence and Data Science (ICCIDS)* Janakpuri, New Delhi. 132, 1441-1448, https://doi: 10.1016/J.Procs.2018.05.076

Ashraf M., Arif S., Basit, A. (2018). Provisioning Quality of Service for Multimedia Applications in Cloud Computing. *International Journal of Information Technology and Computer Science (IJITCS*), 10(5), 40-47 https://doi:10.5815/ijitcs.2018.05.04.

Bahrami, Z., & Tab, F. A. (2016). A New Robust Video Watermarking Algorithm Based on SURF Features and Block Classification. *Springer, Multimedia Tools and Applications*. *77*(1), 327-345. https://doi.org/10.1007/s11042-016-4226-0

Bala, R., & Pal, S. (2021). Image Watermarking Technique for Authenticity. *International Journal of Innovative Research in Technology (IJIRT),* 6(8), pp 230-233. ISSN: 2349-6002

Begum, M., & Uddin, M.S. (2020). Analysis Of Digital Image Watermarking Techniques Through Hybrid Methods. *Journal of Advance in Multimedia,* 2020, pp 1-12, https://doi.org/10.1155/2020/7912690

Beri, R. (2015). Cloud Computing: A Survey on Cloud Computing. *International Journal of Computer Applications,* 11(16), 19-22, https://doi.org/10.5120/19622-1385.

Bhavikatti, S., & Banakar, R. M. (2019). Cloud Service Framework for Multimedia Applications. *International Journal of Electronics Communication and Computer Engineering.* 9(6), 175–180. ISSN: 2249–071X.

Bhuriya, M. D., & Sharma, M. A. (2019). Study on Pros, Cons and Application of Cloud Computing. *International Journal of Research and Analytical Reviews, (IJRAR),* Indore, India, 6(2), 959-964. ISSN: 2349-5138.

Brahim, C., Mohamed, O., Moctar, E., & Konaté, K. (2017). A Survey of Security Challenges in Cloud Computing. *International Conference on Wireless Communications, Signal Processing and Networking (WISPNET)* 1, pp. 843-849. IEEE, doi: 10.1109/WiSPNET.2017.8299880

Calonder, M., Lepetit, V., Ozuysal, M., Trzcinski, T., Strecha, C., & Fua, P. (2011). BRIEF: Computing a local binary descriptor very fast. *IEEE transactions on pattern analysis and machine intelligence*, *34*(7), 1281-1298. https://doi**:** 10.1109/TPAMI.2011.222.

Chythanya, K. R., Kumar, K., Rajesh, M., & Tharun Reddy, S. (2020). Sensor Cloud: A Breakdown Information on The Utilization of Wireless Sensor Network by Means of Cloud Computing. *Journal of Test Engineering and Management*, Telangana, India, 82, pp 13945 – 13954, ISSN: 0193 – 4120.

Embaby, A. Al, Shalaby, M. A. W., & Elsayed, K. M. (2021). Digital Watermarking Properties, Classification and Techniques. *International Journal of Engineering and Advanced Technology (IJEAT)* 9(3), pp2742-2750. https://doi.org/10.35940/ijeat.C5773.029320

Fita, A., & Endebu, B. (2019). Watermarking Colored Digital Image Using Singular Value Decomposition for Data Protection. *Journal of Mathematical and Statistical Analysis.* 2(1), Corpus ID: 162174976.

Garg, P., & Kishore, R. R. (2020). Performance Comparison of Various Watermarking Techniques. Springer Nature, *Multimedia Tools and Applications*, 79(35), 25921-25967. https:// doi:10.1007/S11042-020-09262-1

Gill, A. K., & Varma, A. (2016). Analysis of Watermarking Techniques. *International Journal on Computer Science and Engineering*, India, 8491 pp 153-156 ISSN: 2229-4333.

Goumidi, H., Aliouat, Z., & Harous, S. (2019). Vehicular Cloud Computing Security: A Survey. *Arabian Journal for Science and Engineering*. *45*(4), 2473-2499 https://doi.org/10.1007/s13369-019-04094-0

Gupta, D., & Ahmad, M. (2017). An Efficient Method to Get Improved Peak Signal to Noise Ratio (PSNR), Using Support Vector Machine. *International Journal of Emerging Technology and Advanced Engineering,* 7(9), ISSN 2250-2459

Haris, M., & Khan, R. Z. (2018). A Systematic Review on Cloud Computing. *International Journal of Computer Sciences and Engineering,* 6(11), 632–639. https://doi.org/10.26438/ijcse/v6i11.632639

He, Y., & Hu, Y. (2018). A Proposed Digital Image Watermarking Based on DWT-DCT-SVD 2018 2nd *IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC),* Xi'an, China,1214–1218. https:// doi: 10.1109/IMCEC.2018.8469626.

Ibrahim, I. M., Zeebaree, S., Sadeeq, M. A., Radie, A.H., Shukur, H. M., Jaksi, K., & Rashid, Z. N. (2021). Task scheduling algorithms in cloud computing: A review. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(4), 1041-1053. DOI: https://doi.org/10.17762/turcomat.v12i4.612

Imran, M. (2016). Secure and Robust Adaptive Digital Image Watermarking Methods in Spatial and Wavelet Domains. *A Dissertation submitted to the Department of Electrical & Computer Engineering, Florida State University.* Retrieved from http://purl.flvc.org/fsu/fd/FSU_FA2016_Imran_fsu_0071E_13492

Jadeja, Y., & Modi, K. (2012). Cloud Computing-Concepts, Architecture and Challenges. *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), Nagercoil, India,* pp. 877-880. IEEE. https://doi: 10.1109/ICCEET.2012.6203873.

Jaiswal, R., & Ravi, S. (2018). Robust Imperceptible Digital Image Watermarking Based on Discrete Wavelet & Cosine Transforms Original Image. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* 7(2), 204–213. ISSN: 2278 – 1323.

Ji, L., Patil, G., & Kumar, S. (2020). Robust Digital Watermarking Technique and Process for Digital Content and Image Copyright Protection. *Mukt Shabd Journal*, 9(6), pp 5372-5385, ISSN: 2347-3150.

Joseph, H., & Rajan, B. K. (2020). Image Security Enhancement Using DCT & DWT Watermarking Technique. *International Conference on Communication and Signal Processing (ICCSP), IEEE*, (pp.0940-0945) **doi:**10.1109/ICCSP48568.2020.9182052.

Joshi, A. M., Gupta, S., Girdhar, M., Agarwal, P., & Sarker, R. (2017). Combined DWT–DCT-based video watermarking algorithm using Arnold transform technique. *Proceedings of the international conference on data engineering and communication technology*. 468, (pp. 455-463). Springer, Singapore. https://doi.org/10.1007/978-981-10-1675-2-45.

Juman,T. P. S. (2020). Advantages And Security Challenges of Cloud Computing–Overview. *International Journal of Computer Science and Mobile Computing*, 9(12), 76–85. https://doi.org/10.47760/ijcsmc.2020.v09i12.010

Kadian, P., Arora, S. M., & Arora, N. (2021). Robust Digital Watermarking Techniques for Copyright Protection of Digital Data: A Survey. *Wireless Personal Communications,* Springer, 118(12), 1-25, https://doi.org/10.1007/s11277-021-08177-w

Kaur, J., & Bahl, K. (2018). Cloud Computing–An on-Demand Service Platform and Different Service Models. *International Journal of Innovative Science, Engineering & Technology*, 5(2), 92-96. ISSN: 2348 – 7968.

Kaur, S. (2017). Enhanced Image Watermarking Technique using Wavelets and Interpolation. *International Journal of Image, Graphics and Signal Processing,* Punjab, India, (7) 23–35. https://doi.org/10.5815/ijigsp.2017.07.03.

Khajanchi, N. (2019). To Apply Watermarking Technique in Cloud Computing to Enhance Cloud Data Security. *International Journal of Scientific Development and Research (IJSDR),* 4(7), 237–244. ISSN: 2455-2631.

Khan, D. M., Rao, T. A., & Shahzad, F. (2019). Challenges of Confidentiality and Security in Mobile Cloud Computing and Protective Measures. *Global Regional Review,* 4(I), 154–163. https://doi.org/10.31703/grr.2019(iv-i).18.

Kortli, Y., Jridi, M., Falou, A. Al, & Atri, M. (2020). Face Recognition Systems: A Survey. Saudi Arabia, *2020 Sensors Journal*, *20*(2), 342, https://doi.org/10.3390/s20020342.

Krishnadoss, P., Pradeep, N., Ali, J., Nanjappan, M., Krishnamoorthy, P., & Kedalu Poornachary, V. (2021). Hybrid Cuckoo Crow Search Algorithm (CCSA) for Task Scheduling in Cloud Computing. *International Journal of Intelligent Engineering and Systems*, 14(4), 241-250. https://doi.org/10.22266/ijies2021.0831.22.

Kumar, K., & Singh, V. (2019). Reverse Watermarking Technique to Enhance Cloud Data Security. *Journal of Emerging Technologies and Innovative Research (JETIR).* 6(6), 186-195, ISSN:2349-5162.

Kumar, P. (2018). Digital Video Watermarking: Issues and Challenges. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 7(4), 400–405. ISSN: 2278 – 1323

Kumar, S., Singh, B. K., & Yadav, M. (2020). A Recent Survey on Multimedia and Database Watermarking. Springer, *Multimedia Tools and Applications*, 79(27), 20149-20197. https://doi.org/10.1007/s11042-020-08881-y.

Kumari, Y. (2017). Survey on Digital Image Watermarking & Techniques. *International Journal of Engineering and Computer Science (IJECS).* 6(6) pp21708-21712. https://doi.Org/10.18535/Ijecs/V6i6.25

Lande, K. M. (2019). Survey of Digital Watermarking Techniques and Its Application. *International Research Journal of Engineering and Technology (IRJET)* Navi Mumbai. 6(6) 437–441, ISSN: 2395-0056.

Lee, B. H., Dewi, E. K., & Wajdi, M. F. (2018). Data Security in Cloud Computing Using AES Under HEROKU Cloud. *2018 27th Wireless and Optical Communication Conference (WOCC)* Hualien, Taiwan (pp.1-5). IEEE. https://doi.org/10.1109/WOCC.2018.8372705.

Li, Y. M., Wei, D., & Zhang, L. (2021). Double-encrypted watermarking algorithm based on cosine transform and fractional Fourier transform in invariant wavelet domain. *Information Sciences*, *551*, 205–227. https://doi.org/10.1016/j.ins.2020.11.020

Madhavi, K., Rajesh, G., & Priya, K. S. (2019). A Secure and Robust Digital Image Watermarking Techniques. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 12(8), 2758–2761. https://doi.org/10.35940/ijitee.L2563.1081219

Malik, G., & Kumar, T. (2016). Analysis of Watermarking Techniques. *International Journal of Computer Applications*, 138(10), 30–32. https://doi.org/10.5120/ijca2016908976

Malik, M. I., Wani, S. H., & Rashid, A. (2018). Cloud Computing-Technologies. *International Journal of Advanced Research in Computer Science*, *9*(2). doi: http://dx.doi.org/10.26483/ijarcs.v9i2.5760

Meg, D. (2022). Architecture Of a Fake News Detection System Combining Digital Watermarking, Signal Processing, And Machine Learning. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 13(1), 33–55. https://doi.Org/10.22667/JOWUA.2022.03.31.033

Menendez-Ortiz, A., Feregrino-Uribe, C., Hasimoto-Beltran, R., & Garcia-Hernandez, J. J. (2019). A Survey on Reversible Watermarking for Multimedia Content: A Robustness Overview. *IEEE Access*, (7), 132662-132681. https://doi: 10.1109/ACCESS.2019.2940972

Mohammed, B., Hasan, S., Ameen, S. Y., Mohammed, O., & Hasan, S. (2021). Image Authentication Based on Watermarking Approach: Review. *Asian Journal of Research in Computer Science*, 9(3), 34–51.

https://doi.org/10.9734/AJRCOS/2021/v9i330224.

Namasudra, S, & Pradesh, U. (2018). Cloud Computing: A New Era, Research Article. *Journal of Fundamental and Applied Sciences*. 10(2), 113-135 doi: http://dx.doi.org/10.4314/jfas.v10i2.9.

Navneet, S., & Shailendra, S. (2013). The Amalgamation of Digital Watermarking & Cloud Watermarking for Security Enhancement in Cloud Computing. *International Journal of Computer Science and mobile computing (IJCSMC)*, 2(4), pp 333–339, ISSN: 2320–088X.

Nazir, R., Ahmed, Z., Ahmad, Z., Shaikh, N., Laghari, A., & Kumar, K. (2020). Cloud Computing Applications: A Review. *Journal of EAI Endorsed Transactions on Cloud Systems*, Karachi, Pakistan 6(17), pp164667. https://doi.org/10.4108/eai.22-5-2020.164667.

Noor, T. H., Zeadally, S., Alfazi, A., & Sheng, Q. Z. (2018). Journal of Network and Computer Applications Mobile cloud computing: Challenges and future research directions. *Journal of Network and Computer Applications*, 115(4), 70–85. https://doi.org/10.1016/j.jnca.2018.04.018.

Pal, P., Singh, H. V., & Verma, S. K. (2018). Study on Watermarking Techniques in Digital Images. *2018 Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 1, pp372–376 IEEE. https://doi:10.1109/ICOEI.2018.8553743.

Puppala, S. S., Pabba, S. S., Kasarla, K. S., & Anvitha, K. (2020). Image Segmentation Based Hybrid Watermarking Algorithm For copyright protection. *11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* pp.1-6. IEEE. https://doi:10.1109/ICCCNT49239.2020.9225668.

Ramesh, N., Nagaveni, B., & Satyavathi, P. (2012). An Efficient Technique to provide Security for Data Owners in Cloud Computing. *International Journal of Engineering Research and Technology (IJERT)*, India, 1(5), 1–9. ISSN:2278-0181

Rashid, A., & Chaturvedi, A. (2019). Cloud Computing Characteristics and Services: A Brief Review, *International Journal of Computer Sciences and Engineering*, 7(2), pp 421-426, https://doi.org/10.26438/ijcse/v7i2.421426.

Rashid, A., (2016). Digital watermarking applications and techniques: A Brief Review. *International Journal of Computer Applications Technology and Research*, 5(3), 147-150. ISSN:2319–8656.

Rawat, R., Kaushik, N., & Tiwari, S. (2016). Digital Watermarking Techniques. *International Journal of Advanced Research Computer Communication Engineering*, 5(4), 491-495, https://doi.org/10.17148/IJARCCE.2016.54123.

Ray, A., & Roy, S. (2020). Recent Trends in Image Watermarking Techniques for Copyright Protection: A Survey. (9), **pp** 249–270 *International Journal of Multimedia Information Retrieval*. Springer, https://doi.org/10.1007/s13735-020-

00197-9

Razzaq, M. A., Shaikh, R. A., Baig, M. A., & Memon, A. A. (2017). Digital Image Security: Fusion of Encryption, Steganography and Watermarking. *International Journal of Advanced Computer Science and Applications, (IJACSA)*. 8(5), 224-228. https://doi: 10.14569/IJACSA.2017.080528.

Sahin, A., & Guler, I. (2021). A Survey of Digital Image Watermarking Techniques Based on Discrete Cosine Transform. *International Journal of Information Security Science*, 10(3), pp.99-110. https//doi.ijiss.org/ijiss/index.php/ijiss/article/view/1110.

Sahu, M. I., & Pandey, U. S. (2018). Mobile Cloud Computing: Issues and Challenges. *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, India, *IEEE*, 247–250. https://doi.org/10.1109/ICACCCN.2018.8748376.

Salunkhe, A. (2020). The Review of Cloud Computing System. *International Journal of Advance and Innovative Research.* 7 (1), pp123-127, ISSN 2394 - 7780.

Sarwar, M. U., Hanif, M. K., Talib, R., Sarwar, B., & Hussain, W. (2017). Data Provenance for Cloud Computing Using Watermark. *International Journal of Advanced Computer Science and Applications, (IJACSA)*. 8(6), pp 407-411 https://doi: 10.14569/IJACSA.2017.080654

Sasi, J. P., & Arul, P. (2019). A Study on Digital Watermarking Techniques. *International Journal of Research in Engineering, Science and Management.* 2 (7), pp 490-493, ISSN: 2581-5792.

Savaridass, M. P., Deepika, R., Aarnika, R., Maniraj, V., Gokilanandhi, P., & Kowsika, K. (2021). Digital Watermarking for Medical Images Using DWT and SVD Technique. *IOP Conference Series: Materials Science and Engineering* 1084, (1), pp 012034, https://doi.org/10.1088/1757899X/1084/1/012034

Selvakumari, J., & Jeyaraj, S. (2018). Using Visible and Invisible Watermarking Algorithms for Indexing Medical Images. *The International Arab Journal of Information Technology*, 15(4), 748–755.

Series, I. O. P. C., & Science, M. (2018). *Analysis of the Mean Absolute Error (MAE) and the Root Mean Square Error (RMSE) in Assessing Rounding Model Analysis of the Mean Absolute Error (MAE) and the Root Mean Square Error (RMSE) in Assessing Rounding Model*. *Conference Series: Materials Science and Engineering.* 324(2018). https://doi.org/10.1088/1757-899X/324/1/012049

Singh, J., & Dhiman, G. (2021). A Survey on Cloud Computing Approaches. *Elsevier, Materials Today: Proceedings,* Punjab, India, pp 1-4, https://doi.org/10.1016/j.matpr.2021.05.334.

Singh, N., Joshi, S., & Birla, S. (2019). Suitability of Singular Value Decomposition for Image Watermarking. *2019 6th International Conference on Signal Processing and Integrated Networks, (SPIN),* India, pp983–986. https://doi.org/10.1109/SPIN.2019.8711749.

Singh, R., Ashok, A., & Saraswat, M. (2020). Optimized Robust Watermarking Technique Using CKGSA in DCT-SVD Domain. Elsevier, *Journal of Information Security and Applications*, *14*(10), pp 2052-2063 https://doi.org/10.1049/iet-ipr.2019.1059.

Soni, M., & Kumar, D. (2020). Wavelet-Based Digital Watermarking Scheme for Medical Images. *2020* 12th *International Conference on Computational Intelligence and Communication Networks (CICN)*, pp 403-407. IEEE. https://doi: 10.1109/CICN49253.2020.9242626.

Soualmi, A., Alti, A., & Laouamer, L. (2020). A Novel Blind Watermarking Approach for Medical Image Authentication Using Mineigen Value Features. *Springer Multimedia Tools and Applications*. *80*(2), 2279-2293 https://doi:10.1007/s11042-020-09614-x.

Souley, B., & Adamu, I. A. (2017). An Enhanced Data Integrity Model in Mobile Cloud Environment Using Digital Signature Algorithm and Robust Reversible Watermarking. *International Journal of Scientific & Technology Research*. 6(10), 152–156. ISSN: 2277-8616.

Sowmya, S., Karanth, S., & Kumar, S. (2021). Protection of Data Using Image Watermarking Technique. *Elsevier, Global Transitions Proceedings*. 2(2), pp 386-391. https://doi.org/10.1016/j.gltp.2021.08.035.

Srivastava, A. K., Yadav, D. K., & Pandey, S. K. (2019). The Security in Private Cloud Computing. *International Journal of Communication and Computer Technologies (IJCCT),* 1(2), 119-119. ISSN: 2278-9723.

Srivastava, R., Tomar, R., Gupta, M., Yadav, K.A., & Park, J. (2021). Image Watermarking Approach Using a Hybrid Domain Based on Performance Parameter Analysis. *Information on Multidisciplinary Digital Publishing Institute (MDPI)* 2021, 12, (8), pp 310. https:// doi.org/10.3390/info12080310

Srivastava, P., & Khan, R. (2018). A Review Paper on Cloud Computing. *International Journals of Advanced Research in Computer Science and Software Engineering*, Uttar Pradesh, India 8(6), pp 17-20. ISSN: 2277-128X.

Su, Q., Liu, D., Yuan, Z., Wang, G., Zhang, X., Chen, B., & Yao, T. A. O. (2019). New Rapid and Robust Color Image Watermarking Technique in Spatial Domain. *IEEE Access*, 7, 30398–30409. https://doi.org/10.1109/ACCESS.2019.2895062.

Sujan, S., & Devi, R. K. (2015). A Batchmode Dynamic Scheduling Scheme for cloud computing. *Proceedings of 2015 Global Conference on Communication Technologies (GCCT)* pp 297-302. IEEE. doi: 10.1109/GCCT.2015.7342671.

Suyel, N., Chakraborty, R., Majumder, A., & Moparthi, N. R. (2021). Securing Multimedia by Using DNA-Based Encryption in the Cloud Computing Environment. *ACM Transactions on Multimedia Computing, Communications and Applications,* India, 16(3) pp 1–19. https://doi.org/10.1145/3392665.

Taghipour, M., & Mahboobi, M. (2020). Application of Cloud Computing in System Management in Order to Control the Process. *ITS Journal,* Tehran, Iran, *3*(3), 34- 55. https://doi.org/10.31058/j.mana.2020.33003.

Tan, S. Y., Arshad, H., & Abdullah, A. (2019). Distinctive Accuracy Measurement of

Binary Descriptors in Mobile Augmented Reality. *Journal of the National Center for Biotechnology Information,* Malaysia, 14(1), e0207191, https://doi.org/10.1371/journal.pone.0207191.

Tanash, R. M., Khalifeh, A. F., & Darabkh, K. A. (2019). Communication over cloud computing: A security survey. *IEEE 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics, (MIPRO),* Croatia, 496–501. https://doi.org/10.23919/MIPRO.2019.8756926.

Tanwar, L. (2018). Review of Different Transforms used in Digital Image Watermarking. *2018 2nd IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES),* 1165–1171. https://doi:10.1109/ICPEICES.2018.8897456.

Thaiyalnayaki, S., & Devi, S. (2018). Protection of Data in Cloud Computing Using Image Processing Watermarking Technique. *International Journal of Computer Sciences and Engineering.* 6(11), 115–118. E-ISSN: 2347-2693.

Thanki, R., Dwivedi, V., & Borisagar, K. (2017). Multimedia Data. *Journal of King Saud University Computer and Information Sciences*. *31*(4), 436-451 https://doi.org/10.1016/j.jksuci.2017.05.005.

Uma, B., & Sumathi, S. (2017). A Survey About Cloud Computing and an Improved Method of Data Security Using Watermarking Technique with RSA Algorithm in Cloud Environment. *Asian Journal of Research in Social Sciences and Humanities,* 7(5), 325-336. https://doi: 10.5958/2249-7315.2017.00319.7

Vo, P. H., Nguyen, T. S., Huynh, V. T., & Do, T. N. (2017). A Robust Hybrid Watermarking Scheme Based on DCT and SVD for Copyright Protection of Stereo Images. *IEEE 2017 4th NAFOSTED Conference on Information and Computer Science,* Hanoi, Vietnam, (pp. 331-335). IEEE. https://doi: 10.1109/NAFOSTED.2017.8108087.

Vybornova, Y. (2020). A New Watermarking Method for Video Authentication with Tamper Localization. *International Conference on Computer Vision and Graphics,* Springer, Cham. 12334, pp. 201-213, https://doi.org/10.1007/978-3-030-59006-2_18.

Wadhera, S., Kamra, D., Rajpal, A., Jain, A., & Jain, V. (2022). A Comprehensive Review on Digital Image Watermarking. *Journal on Computer Networks and Communications,* Chennai, India, 9976, pp 0-2 https://doi.org/10.48550/arXiv.2207.06909.

Wang, R., Zhang, W., Shi, Y., Wang, X., & Cao, W. (2019). GA-ORB: A New Efficient Feature Extraction Algorithm for Multispectral Images Based on Geometric Algebra. *IEEE Access*, China, 7, 71235–71244. https://doi.org/10.1109/ACCESS.2019.2918813

Wang, T., Wang, Z., Cao, Y., Wang, Y., & Hu, S. (2021). A Multi-BRIEF-Descriptor Stereo Matching Algorithm for Binocular Visual Sensing of Fillet Welds with Indistinct Features. *Journal of Manufacturing Processes*, 66(2), 636–650. https://doi.org/10.1016/j.jmapro.2021.04.031

Wazirali, R., Ahmad, R., Al-amayreh, A., Al-madi, M., & Khalifeh, A. (2021). Secure Watermarking Schemes and Their Approaches in the IoT Technology: An Overview. *10*(14), 1744. *2021 Journal of MDPI Electronics*, Saudi Arabia, https://doi.org/10.3390/electronics10141744.

Yadav, D., & Sharma, A. (2019). Creation of Virtual World with the Evolution of Cloud Computing. *International Journal of Research in Engineering, Science and Management*, India, 2(9), pp 199-202, ISSN: 2581-5792.

Yang, G., Jan, M. A., & Member, S. (2020). Interoperability and Data Storage in Internet of Multimedia Things: Investigating Current Trends, Research Challenges and Future Directions. *IEEE Access*, 8, pp(124382-124401). IEEE. https://doi.org/10.1109/ACCESS.2020.3006036.

Yu, X., Wang, C., & Zhou, X. (2019). A Hybrid Transforms-Based Robust Video Zero-Watermarking Algorithm for Resisting High Efficiency Video Coding Compression. *IEEE Open Access Journal*, 7, 2019, pp 115708-115724. IEEE. https://doi: 10.1109/ACCESS.2019.2936134.

Zhang, J., Liu, X., & Liu, X. (2015). Design of Binary Robust Independent Elementary Features through Compressive Sensing View. *International Journal of Applied Physics and Mathematics* 5(1). https:// doi: 10.17706/ijapm.2015.5.1.67-75

APPENDICES

Appendix: Implementation code of Brief,Svd,Dwt in Python, Anaconda

```
import numpy as np
import cv2
import pywt
import random
import math
import cmath
from matplotlib import pyplot
import matplotlib.pyplot as plt
from skimage.metrics import structural_similarity as ssim
from dwt_svd import DWT_SVD
from dwt import DWT
from brief import BRIEF
from brief_svd import BRIEF_SVD
from svd import SVD
from brief_dwt import BRIEF_DWT
from performance_metrics import psnr,mse,snr,mae
import random
if__name__== "_main_":
    SavedImage = ("Image"+ str(random.randint(0,999))+".jpg")
    print(SavedImage)
    coverImage = cv2.imread('cover/image5.jpg',0)
    watermarkImage = cv2.imread('watermark/watermark.png',0)
    BRIEF_DWT(coverImage,watermarkImage,SavedImage)
    result = cv2.imread(SavedImage,0)
    coverImage = cv2.resize(coverImage,(512,512))
    path1 = 'cover/image1.jpg'
    path2 = SavedImage
    print(path2)

    x=psnr(coverImage,result)
    print('Peak Signal to Noise Ratio =',x)
    y = mse(coverImage,result)
    print('Mean Squared Error = ',y)
    z = snr(coverImage,result)
    print('Signal to Noise Ratio = ', z)
    u = mae(coverImage,result)
    print('Compute Mean Absolute Error = ', u)

    # setup the figure
    fig = plt.figure("Orignal Image Vs Watermarked Image")
    plt.suptitle("PSNR: %.2f, MSE: %.2f,SNR: %.2f,MAE: %.2f" % (x, y, z,u))
        # show first image
    ax = fig.add_subplot(1, 2, 1)
    plt.imshow(coverImage, cmap = plt.cm.gray)
    plt.axis("off")
        # show the second image
```

```
    ax = fig.add_subplot(1, 2, 2)
    plt.imshow(result, cmap = plt.cm.gray)
    plt.axis("off")
        # show the images
    plt.show()

    cv2.waitKey(0)
    cv2.destroyAllWindows()

    import numpy as np
import cv2
import pywt
import random
import math
import cmath
from matplotlib import pyplot
import matplotlib.pyplot as plt
from skimage.metrics import structural_similarity as ssim
from dwt_svd import DWT_SVD
from dwt import DWT
from brief import BRIEF
from brief_svd import BRIEF_SVD
from svd import SVD
from brief_dwt import BRIEF_DWT
from performance_metrics import psnr,mse,snr,mae
import random
if__name__== "_main_":
    SavedImage = ("Image"+ str(random.randint(0,999))+".jpg")
    print(SavedImage)
    coverImage = cv2.imread('cover/image3.jpg',0)
    watermarkImage = cv2.imread('watermark/watermark.png',0)
    BRIEF(coverImage,SavedImage)
    result = cv2.imread(SavedImage,0)
    coverImage = cv2.resize(coverImage,(512,512))
    path1 = 'cover/image1.jpg'
    path2 = SavedImage
    print(path2)

    x=psnr(coverImage,result)
    print('PSNR =',x)
    y = mse(coverImage,result)
    print('MSE = ',y)
    z = snr(coverImage,result)
    print('SNR = ', z)
    u = mae(coverImage,result)
    print('MAE = ', u)

    # setup the figure
    fig = plt.figure("Orignal Image Vs Watermarked Image")
    plt.suptitle("PSNR: %.2f, MSE: %.2f,SNR: %.2f,MAE: %.2f" % (x, y, z,u))
```

```
        # show first image
    ax = fig.add_subplot(1, 2, 1)
    plt.imshow(coverImage, cmap = plt.cm.gray)
    plt.axis("off")
        # show the second image
    ax = fig.add_subplot(1, 2, 2)
    plt.imshow(result, cmap = plt.cm.gray)
    plt.axis("off")
        # show the images
    plt.show()


    cv2.waitKey(0)
    cv2.destroyAllWindows()

       import numpy as np
import cv2
import pywt
import random
import math
import cmath
from matplotlib import pyplot
import matplotlib.pyplot as plt
from skimage.metrics import structural_similarity as ssim
from dwt_svd import DWT_SVD
from dwt import DWT
from brief import BRIEF
from brief_svd import BRIEF_SVD
from svd import SVD
from brief_dwt import BRIEF_DWT
from performance_metrics import psnr,mse,snr,mae
import random
if__name__== "_main_":
    SavedImage = ("Image"+ str(random.randint(0,999))+".jpg")
    print(SavedImage)
    coverImage = cv2.imread('cover/image10.jpg',0)
    watermarkImage = cv2.imread('watermark/watermark.png',0)
    BRIEF_SVD(coverImage,watermarkImage,SavedImage)
    result = cv2.imread(SavedImage,0)
    coverImage = cv2.resize(coverImage,(512,512))
    path1 = 'cover/image1.jpg'
    path2 = SavedImage
    print(path2)

    x=psnr(coverImage,result)
    print('PSNR =',x)
    y = mse(coverImage,result)
    print('MSE = ',y)
    z = snr(coverImage,result)
    print('SNR = ', z)
```

```
    u = mae(coverImage,result)
    print('MAE = ', u)

    # setup the figure
    fig = plt.figure("Orignal Image Vs Watermarked Image")
    plt.suptitle("PSNR: %.2f, MSE: %.2f,SNR: %.2f,MAE: %.2f" % (x, y, z,u))
            # show first image
    ax = fig.add_subplot(1, 2, 1)
    plt.imshow(coverImage, cmap = plt.cm.gray)
    plt.axis("off")
            # show the second image
    ax = fig.add_subplot(1, 2, 2)
    plt.imshow(result, cmap = plt.cm.gray)
    plt.axis("off")
            # show the images
    plt.show()


    cv2.waitKey(0)
    cv2.destroyAllWindows()


    import numpy as np
import cv2
import pywt
import random
import math
import cmath
from matplotlib import pyplot
import matplotlib.pyplot as plt
from skimage.metrics import structural_similarity as ssim
from dwt_svd import DWT_SVD
from dwt import DWT
from brief import BRIEF
from brief_svd import BRIEF_SVD
from svd import SVD
from brief_dwt import BRIEF_DWT
from performance_metrics import psnr,mse,snr,mae
import random
if__name__== "_main_":
    SavedImage = ("Image"+ str(random.randint(0,999))+".jpg")
    print(SavedImage)
    coverImage = cv2.imread('cover/image10.jpg',0)
    watermarkImage = cv2.imread('watermark/watermark.png',0)
    DWT(coverImage,watermarkImage,SavedImage)
    result = cv2.imread(SavedImage,0)
    coverImage = cv2.resize(coverImage,(512,512))
    path1 = 'cover/image1.jpg'
    path2 = SavedImage
    print(path2)
```

```
    x=psnr(coverImage,result)
    print('PSNR =',x)
    y = mse(coverImage,result)
    print('MSE = ',y)
    z = snr(coverImage,result)
    print('SNR = ', z)
    u = mae(coverImage,result)
    print('MAE = ', u)

    # setup the figure
    fig = plt.figure("Orignal Image Vs Watermarked Image")
    plt.suptitle("PSNR: %.2f, MSE: %.2f,SNR: %.2f,MAE: %.2f" % (x, y, z,u))
        # show first image
    ax = fig.add_subplot(1, 2, 1)
    plt.imshow(coverImage, cmap = plt.cm.gray)
    plt.axis("off")
        # show the second image
    ax = fig.add_subplot(1, 2, 2)
    plt.imshow(result, cmap = plt.cm.gray)
    plt.axis("off")
        # show the images
    plt.show()


    cv2.waitKey(0)
    cv2.destroyAllWindows()


    import numpy as np
import cv2
import pywt
import random
import math
import cmath
from matplotlib import pyplot
import matplotlib.pyplot as plt
from skimage.metrics import structural_similarity as ssim
from dwt_svd import DWT_SVD
from dwt import DWT
from brief import BRIEF
from brief_svd import BRIEF_SVD
from svd import SVD
from brief_dwt import BRIEF_DWT
from performance_metrics import psnr,mse,snr,mae
import random
if__name__== "_main_":
    SavedImage = ("Image"+ str(random.randint(0,999))+".jpg")
    print(SavedImage)
    coverImage = cv2.imread('cover/image10.jpg',0)
```

```
    watermarkImage = cv2.imread('watermark/watermark.png',0)
    DWT_SVD(coverImage,watermarkImage,SavedImage)
    result = cv2.imread(SavedImage,0)
    coverImage = cv2.resize(coverImage,(512,512))
    path1 = 'cover/image1.jpg'
    path2 = SavedImage
    print(path2)

    x=psnr(coverImage,result)
    print('PSNR =',x)
    y = mse(coverImage,result)
    print('MSE = ',y)
    z = snr(coverImage,result)
    print('SNR = ', z)
    u = mae(coverImage,result)
    print('MAE = ', u)

    # setup the figure
    fig = plt.figure("Orignal Image Vs Watermarked Image")
    plt.suptitle("PSNR: %.2f, MSE: %.2f,SNR: %.2f,MAE: %.2f" % (x, y, z,u))
        # show first image
    ax = fig.add_subplot(1, 2, 1)
    plt.imshow(coverImage, cmap = plt.cm.gray)
    plt.axis("off")
        # show the second image
    ax = fig.add_subplot(1, 2, 2)
    plt.imshow(result, cmap = plt.cm.gray)
    plt.axis("off")
        # show the images
    plt.show()


    cv2.waitKey(0)
    cv2.destroyAllWindows()


    import numpy as np
import cv2
import pywt
import random
import math
import cmath
from matplotlib import pyplot
import matplotlib.pyplot as plt
from skimage.metrics import structural_similarity as ssim
from dwt_svd import DWT_SVD
from dwt import DWT
from brief import BRIEF
from brief_svd import BRIEF_SVD
from svd import SVD
```

```
from brief_dwt import BRIEF_DWT
from performance_metrics import psnr,mse,snr,mae
import random
if__name__== "_main_":
    SavedImage = ("Image"+ str(random.randint(0,999))+".jpg")
    print(SavedImage)
    coverImage = cv2.imread('cover/image3.jpg',0)
    watermarkImage = cv2.imread('watermark/watermark.png',0)
    SVD(coverImage,watermarkImage,SavedImage)
    result = cv2.imread(SavedImage,0)
    coverImage = cv2.resize(coverImage,(512,512))
    path1 = 'cover/image1.jpg'
    path2 = SavedImage
    print(path2)

    x=psnr(coverImage,result)
    print('PSNR =',x)
    y = mse(coverImage,result)
    print('MSE = ',y)
    z = snr(coverImage,result)
    print('SNR = ', z)
    u = mae(coverImage,result)
    print('MAE = ', u)

    # setup the figure
    fig = plt.figure("Orignal Image Vs Watermarked Image")
    plt.suptitle("PSNR: %.2f, MSE: %.2f,SNR: %.2f,MAE: %.2f" % (x, y, z,u))
        # show first image
    ax = fig.add_subplot(1, 2, 1)
    plt.imshow(coverImage, cmap = plt.cm.gray)
    plt.axis("off")
        # show the second image
    ax = fig.add_subplot(1, 2, 2)
    plt.imshow(result, cmap = plt.cm.gray)
    plt.axis("off")
        # show the images
    plt.show()

    cv2.waitKey(0)
    cv2.destroyAllWindows()
```