Multimedia Tools and Applications (2022) 81:21417–21448
https://doi.org/10.1007/s11042-022-12550-7

A cloud-based buyer-seller watermarking protocol (CB-BSWP) using semi-trusted third party for copy deterrence and privacy preserving

Ashwani Kumar[1]

Received: 15 August 2020 / Revised: 25 January 2022 / Accepted: 31 January 2022 /
Published online: 15 March 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
Nowadays, cloud computing provides a platform infrastructure for the secure dealing of digital data, but privacy and copy control are the two important issues in it over a network. Cloud data is available to the end user and requires enormous security and privacy techniques to protect the data. Moreover, the access control mechanism with encryption-based technique protects the digital rights for participants in a transaction, but they do not protect the media from being illegally redistributed and do not restrict an authorized user to reveal their secret information this is referred to as you can access but you cannot leak. This brought out a need for controlling copy deterrence and preserving the privacy of digital media over the internet. To overlook this, we proposed a cloud-based buyer-seller watermarking protocol (CB-BSWP) with the use of a semi-trusted third party for copy deterrence and privacy-preserving in the cloud environment. The suggested scheme uses 1) a privacy homomorphism cryptosystem with Diffie-Hellman key exchange algorithm to provide an encrypted domain for the secure exchange of digital media 2) adopt robust and fair watermarking techniques to ensure high imperceptibility and robustness for the watermarked images against attacks 3) two services of cloud Infrastructure as a service (IaaS) to support virtualized computing infrastructure and Watermarking as a service (WaaS) to execute the speedy process of watermarking, this process is supported by watermarking generation and signing phase (WGSP) and watermark extraction and verifying phase reported in 4th section. 4) cloud service provider (CSP) considered as a "semi-trusted" third party to reduce the burden from the trusted third party (TTP) server and provide storage for the encrypted digital media on cloud databases, this frees content owner from not having a separate storage infrastructure. The proposed scheme encrypts the digital content by using SHA-512 algorithm with key size 512-bits to ensure that it doesn't affect computational time during

✉ Ashwani Kumar
ashwani.kumarcse@gmail.com

[1] Department of Computer Science & Engineering (AIML), Sreyas Institute of Engineering and Technology, Hyderabad 500068, India

the process of encryption. The suggested scheme addresses the problems of piracy tracing, anonymity, tamper resistance, non-framing, customer rights problem. The role of cloud is crucial because it reduces communication overhead, provides unlimited storage, supports the watermarking process and offers a solution for the secure distribution of end-to-end security of digital content over cloud. To check the performance of the suggested CB-BSWP protocol against common image processing attacks, we have conducted experiments in which the perceptual quality of watermarked digital media was found enhanced, resulting in a robust watermark.

Keywords Access control · Cloud computing environment · Copy deterrence · Infrastructure provider · Privacy-preserving tamper resistance

1 Introduction

The rapid development of cloud computing technologies, in the current scenario is the reason behind the increase in the use of digital data over the cloud. Many cloud service providers now started to bring effective cloud services to attract users. The risk of redistribution of multimedia content increases as the rapid use of cloud computing technology. Therefore, there is a need for copyright protection and digital watermarking technique for multimedia data. Based on the recent literature, we can conclude that digital watermarking has turn into a promising technique to protect the copyrights for the buyer and seller. It plays a key role to provide the digital rights for the participants involving in a transaction. The prime aim of watermarking is to protect the copyrights and embedded information for the original data [1]. The Popularity of the internet has some bad consequences such as illegal copying, redistribution, duplication of digital data by using the advanced software and tools freely available in the market. The robust and fair watermarking based methods integrate asymmetric key cryptosystem with fingerprinting based watermarking to ensure rights for the content owner and the customer [2]. Fingerprinting and copy control techniques are two important pillars for a digital right management (DRM) system. They require high robustness, adequate security, and high perceptual quality for the embedded watermarks and watermarked images. DRM system is expected to protect the digital media from being illegally copied, edited, and redistributed. Memon et al. [3] proposed an efficient method to divide the watermarks into various groups. In reality, deceptive web users or social networks and website administrators always have the advantage to obtain the duplicate multimedia content such as pictures, animations, videos from the authorized subscribers. This multimedia content may be redistributed or manipulated, hence destroying their rightful owners' reputation, or exposing their secret data. This motivates the authors to provide an effective solution for addressing such problems and ensures adequate security, copyright protection in the cloud computing environment [4]. However, implementing an access control mechanism alone would not be sufficient to protect media sharing for the service providers. Robust and fair watermarking methods required the following properties [5, 6].

- Robustness: This refers to the sustainability of the watermark. A watermark is the most important component in digital watermarking. Thus, it must stand, general image processing attacks such as filtering, the summation of noise, rotation, insertions and cropping. The watermark should also stand against the manipulation of data. In other words, one can refer that inserted watermark should survive against different types of multimedia attacks. In

any case, the adversary should not have knowledge of watermark, embedded into the media.

- Protection: All the images should be distributed into the cloud in an encrypted form. These images could be watermarked images and can be end users secret information. The watermarking system should have a protecting wrapper before the outsourcing of digital data.
- Capacity: Refer to the amount of watermark information inserted into the cover object. The watermarking system should allow more amount of data to be inserted in the cover media. This property of the digital right management system enables a content owner to embed more watermarking information, which helps to trace the pirated copies.
- Perceptual Quality: This property refers to maintaining a high quality of the watermarked image even though more watermark information is present in the cover image. The prime aim of any watermarking scheme is to produce identical images.
- Reliability: The reliability can be achieved if the watermarking system ensures that the scheme is enabled with a tamper resistant device and is collusion resistant. Tamper resistant devices must protect the stealing of digital content from unauthorized users.
- Scalability: Scalability refers to the adaptability of a watermarking system even with the increase of participants such as content owner or distributor at runtime. The system should be flexible even though the size of the network increases.
- Effectiveness: The scheme should be effective for the insertion and extraction of the watermark from the multimedia content. The amount of time needed to fix the security measures before the distribution of digital media should be abstract and minimal.

2 Motivation and contribution

Our research work is influenced by the Johan Bjorklund [7] study where the participants are considered a vital component of the welfare of human and liberty. John provides a solution for the content owner to publish their multimedia data, without the use of TTP, but this approach does not use robust watermarking. John's research work is motivated by Boneh et al. who enables the content owner to launch the services on un-trusted clouds [8]. The following are key points of motivation.

1) CSP provides ubiquitous computing for accessing the cloud anytime from anywhere and renders the best possible service to its user.
2) To address the problem of piracy tracing, copy deterrence, anonymity control and collusion resistance by using a "semi-trusted" third party with a cloud server.
3) To shift the watermarking process from the watermark certificate authority (WCA) towards watermarking as a service (WaaS), which would make protocol fast & efficient.
4) WCA, considered as a trusted third party may become unresponsive as the customers grow into a network this motivates the author to use a system model which is partially TTP free.

The rest of the research article is structured as follows: Section 1 describes the introduction of digital watermarking and cloud computing capabilities. Section 2 brings a brief literature review of recent buyer-seller watermarking protocol with a cloud environment. Section 3 covers the problem formulation of the CB-BSWP. Section 4 provides a detailed description of

CB-BSWP using semi-trusted third party for copy deterrence and privacy-preserving to achieve the goals. Section 5 presents a discussion on the security analysis of CB-BSWP. Section 6 demonstrates performance evaluation of CB-BSWP. The Final section concludes our research article.

3 Related work

The citizens of the EU force many social networking websites importantly "Facebook", "Twitter" and "YouTube" to delete the basic information of thousands of users [9]. However, consumers cannot legally confirm the erasure of data unless they trust their service providers. Nevertheless, cloud storage is becoming increasingly efficient and economical. Despite the prominent advantages, the implementation of the cloud media center deprives the direct influence of service providers over outsourced media services and poses security concerns [10–14]. Incorporating security measures into the cloud is very much-needed because only authorized users should allow accessing the encrypted media. Cloud computing provides a better approach for business level activities including information technology services that depend upon the future and current edge technology [15–18]. Security in the cloud is the most challenging task by the virtue of rise of cloud computing technology. With the increase in the number of users, their expectations in terms of reliability, privacy, scalability, ubiquitous computing and integrity from CSP are also increasing. CSP should gain customer confidence by securing their private data in the cloud and provide consumers with an adequate security mechanism [19]. The security of participants can be achieved by adopting privacy-preserving technology at run time. The cloud data cannot be altered or viewed by an unauthorized user and it should be stored in cloud server in an encrypted form. The privacy should not leak during data transfer from local host machine to Internet data centers. The CSP must have an authentication and authorization mechanism to provide access rights and access control for the users to safeguard the communication. In history, many BSWP published with different technology and techniques. Memon et al. [20] give a solution in which the use of a trusted third party produces an encrypted fingerprint where the encryption is done with the public key of the buyer. Customer's rights problem in BSWP was first introduced by Qiao et al. [21, 22]. Xiaorui Zhang et al. proposed a solution based on ROI and IWT for remote consultation of COVID-19 to avoid cross-infection and regional differences in medical resources. They achieve a remarkable PSNR value 51.24 against noise attacks [23]. I-Ching Hsu et al. gives a solution in his paper XML-based cloud computing ecosystem for deploying, managing and offering services through a shared infrastructure by using web 2.0 mashups as a service, called WMaaS [24]. N. Jayashree et al. proposed a robust image watermarking scheme in which the watermark was embedded by modifying singular values of the host image with the singular values of the watermark image [25]. All the above BSWP protocol does not use the cloud environment as storage infrastructure instead of they, use private infrastructure which requires huge cost of maintaining a server.

We proposed a CB-BSWP using "semi-trusted" third party for copy deterrence and privacy preserving with cloud computing capabilities. Our protocol uses two important services of cloud (1) Infrastructure as a service (IaaS) to support virtualized computing infrastructure over the non-secure channel. (2) Watermarking as a service (WaaS) to support the speedy process of watermarking. Additionally, the scheme adopts privacy homomorphism cryptosystem and Diffie-Hellman key exchange to protect the privacy of the participants over cloud. These two

together create an encrypted environment to ensure a secure exchange of data between buyer and content owner. The reason to use "semi-trusted" third party is to avoid the situation of the trusted third party (TTP) server overloaded. Therefore, the scheme uses a cloud service provider considered as a "semi-trusted" third party to reduce the burden from the TTP server. The CSP act as a trusted signatory, which guarantees: digital rights for the participants, and provides confidentiality, integrity, availability characteristics for participant's data. CSP uses a digital signature certificate associated with buyer's watermark for a transaction. This CSP now holds the encrypted digital media on its cloud databases which refrain the content owner from maintaining a separate storage infrastructure. The scheme uses robust and fair watermarking to ensure high imperceptibility and robustness for the watermarked images. A flexible and secure BSWP should address the following issues [26, 27].

- Anonymity problem (AP): Identity of the buyer should not expose until the buyer is accused as a malicious user in a transaction [5]. The watermarking system should not reveal the information of the buyer to the content owner unless a duplicate copy found.
- Tamper Detection (TD): The watermarking system must detect the modifications to digital content by an unauthorized use. The intruder should not be able to gain the knowledge of watermark information.
- Non-framing problem (NFP): Content owner can frame an innocent buyer by illegally redistributing the buyer's watermark to another buyer. Therefore, the watermarking system should not allow for a false allegation of an innocent buyer [6]. This property comes under the customer right problem.
- Non-repudiation problem (NRP): Non-repudiation simply enables the watermarking system to identify malicious parties denying a transaction. It provides a solution against denying the digital media by either a seller or buyer.
- Customer's rights problem (CRP): The reason to design BSWP was to protect the digital rights of customers. A content owner should not frame an innocent buyer CRP prevents the owner to embed the same watermark for different customers. Additionally, the seller always has the advantage to accuse the customer by inserting his watermark into digital media purchased by a different customer.
- Traceability Problem (TP): The watermarking system can identify the spurious buyer for copyright breaches. The owner of digital media must trace illegal copies and monitors the illegal copying of multimedia content. The buyer may be profited by redistributing the content illegally without the consent of the authorized seller.
- Unbinding problem (UP): Simply refers to creating a robust and invisible watermark for every transaction into the media. The watermarking system must restrict the seller by leaking the private information of the buyer.

3.1 Security requirements for encrypted cloud

The demand for data storage is increasing exponentially with the huge growth in the number of users over the network. Therefore, delivering efficient services to its stakeholders is a challenge for IT companies. For this reason, IT companies rely on cloud-based storage [28]. This cloud storage requires a safeguard for the security of the content owner and buyers in the cloud [29, 30]. The main objective behind moving towards the cloud environment is to provide

effective services for buyers and content owners with the protection of secret information over the cloud without compromising the security concerns. For effective utilization of the cloud environment, the following characteristics are required like on-demand, storage, latency, scalability, fault tolerance, virtualization, resource sharing, Quality-of-Service (QoS) management and ubiquitous computing. Virtualization makes it possible to scale up computing resources on-demand [31]. The proposed CB-BSWP provides a sheltered dealing of digital content over the cloud and ensures the protection of involved participants effectively. Figure 1 represents the requirements for the CB-BSWP. Lu Leng et al. proposed a novel scheme for face and palmprint recognition by making use of DCT domain and dynamic weighted discrimination power analysis. They address the problem of how to select proper DCT coefficients to achieve best discrimination effect. They also pointed out the issue of low recognition rate in their research [32, 33].

A trusted third party is used to guarantee fairness in a transaction between the buyer and the content owner, provide the digital rights for both so that the buyer cannot frame the content owner and vice versa. The disadvantage of using TTP as WCA is the additional processing overhead for every transaction and cost for buyer and content owner. Therefore, we introduced a CB-BSWP with CSP as a "semi-trusted" third party to avoid the partial role of WCA by using a cloud environment still the scheme ensures fairness in a transaction. The scheme uses infrastructure as a service IaaS to support virtualized computing infrastructure over the non-secure channel. This service provides an executing infrastructure, including storage, processing, servers, networks, virtual machine, execution, databases and other resources to the CSP. The processing of watermark is carried out by a service of cloud computing called watermarking as a service WaaS. Our protocol addresses the problems associated with previously published BSWP such as piracy tracing, anonymity control, unbinding, collusion resistance and non-repudiation. The scheme includes a tamper

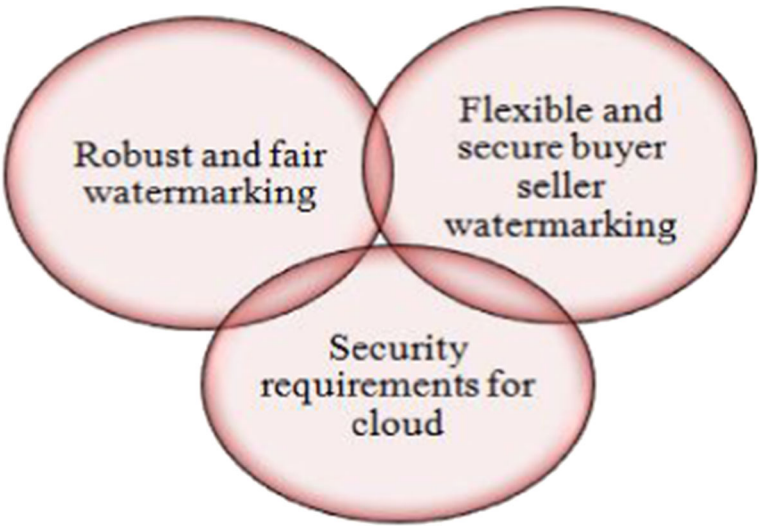


Fig. 1 Requirements for cloud based buyer-seller watermarking protocol (CB-BSWP)

resistant device to protect the stealing of the encrypted digital content from the unauthorized user. The role of cloud services becomes important because they reduce the communication overhead, provide storage and support the speedy process of watermarking. These cloud services, strengthen the suggested protocol and make it secure, flexible fair and effective. Our suggested protocol resolves the problem of privacy-preserving and copy deterrence by identifying the true owner of digital content.

3.2 Our key contributions

The focus of this research work is to protect the secrecy of the participants involved in purchase using a semi-trusted third party for copy deterrence and privacy preservation. The scheme enables an encrypted domain by using the privacy homomorphism cryptosystem and Diffie-Hellman key exchange for the secure transmission of digital content. The key points of our contribution are given below.

1) The use of an encrypted cloud environment in this research, preserves the privacy of the participants and enables secure transmission of digital content.
2) The encrypted cloud environment allows the scheme to perform secure exchange of digital media and helps to identify illegal pirated digital media.
3) The IaaS provides an infrastructure framework for reducing the communication overhead and cost for the content owner. WaaS is used to support the speed up process of watermarking that enables the digital content to achieve high efficiency for embedding & extracting the watermarks.
4) The CB-BSWP uses a fingerprinting based watermarking method to ensure digital rights for the content owner and the customer. It only enables the authorized user to decrypt the digital content using the decryption key is shared between a buyer and content owner.
5) CSP provides an environment in which neither the content owner nor the customer is having full knowledge where exactly the watermark bits are inserted into the digital media which solves many problems associated with BSWP.
6) CSP eliminates the partial role of TTP because the entire watermarking process shifted towards the cloud that makes the scheme independent of TTP. The scheme provides sheltered dealing of digital content over the cloud and protects the security measures of buyers and content owners effectively.

4 Problem formulation

This section presents various requirements to implement the suggested CB-BSWP including shortcomings of previously extended BSWP, robust & fair watermarking, security in the encrypted form and problem of key exchange. Table 1 describes the roles and their meaning used in CB-BSWP.

4.1 System model

In our proposed protocol, we have used the same trust model as used by Memon et al. [20] and Lei et al. [34]. The model involves different entities: the content owner, buyer, cloud service

Table 1 Describes the roles and notations used in CB-BSWP

Symbols	Meaning
$B\rightarrow$	Buyer
$CO\rightarrow$	Content owner
$ARB\rightarrow$	Arbiter
$T\rightarrow$	Timestamp
$ID_{CO}\rightarrow$	Identity of content owner
$ID_B\rightarrow$	Identity of buyer
$X\rightarrow$	Cover object
$X^{r}\rightarrow$	Watermarked cover object
$W\rightarrow$	Watermark
$W^{\tau f}\rightarrow$	Forge watermark
$DM\rightarrow$	Digital media
$SDM\rightarrow$	Suspicious digital media
$XDM\rightarrow$	Watermarked digital media
$Key\rightarrow$	Key
$WCA\rightarrow$	Watermark certificate authority
$CMC\rightarrow$	Cloud media center
$P_H\rightarrow$	Privacy homomorphism
$CS\rightarrow$	Cloud server
$PKI\rightarrow$	Public-key cryptography
$Key_{\mathrm{DH-SHA512}}\rightarrow$	Diffie-Hellman key exchange followed by secure hash algorithm (SHA-512)
$Enc^{N}\rightarrow$	Encryption using the secret key
$Dec^{N}\rightarrow$	Decryption using the secret key
$VerN_{DS}\rightarrow$	Verification of digital signature
$DS\rightarrow$	Digital signature
$Sign_{(user)}\rightarrow$	Signing algorithm for the corresponding user
$S_P\rightarrow$	Spurious buyer
$N\rightarrow$	Nonce in transaction
$Cert_B\rightarrow$	Certificate of buyer
$Cert_{CO}\rightarrow$	Certificate of content owner
$CSP\rightarrow$	Cloud service provider

provider, cloud server, spurious buyer and watermark certification authority. The detailed explanation of these terminologies is discussed in section 4.

4.2 Robust and fair watermarking approach

To achieve great robustness the trust model adopted fingerprinting based digital watermarking techniques which involve a secret key, certificates, public key infrastructure (PKI), arbiter and privacy homomorphism cryptosystem [26, 35].

4.3 Key management

In the key management, the prime objective is how securely the key can be transmitted between content owners and buyer. Once the successful authentication is done, a random key has to be generated for secure communication between the buyer and content owner. Only then, secure digital media can be accessible by the buyer [7]. There is a number of ways available for transmitting a random secret key to a buyer. The Diffie-Hellman key exchange followed by the hash algorithm (SHA-512) is used to exchange the key for secure transmission. In this mathematical computation is applied for generating the random key, which

Step 1) Select two global public elements q and α where q is a prime number and α is a primitive root of q;

- $(\alpha < q)$ and α is a primitive root of q

Step 2) Buyer B key generation takes place as follows.

- Select a private key PRk_B Where $PRk_B < q$
- Calculate public key PUk_B Such that $PUk_B = \alpha^{PRk_B} \bmod q$

Step 3) Content owner CO key generation takes place as follows.

- Select a private key PRk_{CO} Where $PRk_{CO} < q$
- Calculate public key PUk_{CO} Such that $PUk_{CO} = \alpha^{PRk_{CO}} \bmod q$

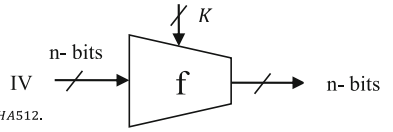
Step 4) Buyer B calculates the secret key.

- $K = (PUk_{CO})^{PRk_B} \bmod q$

Step 5) Content owner CO calculates the secret key.

- $K = (PUk_B)^{PRk_{CO}} \bmod q$

Step 6) Feed this secret key K into SHA-512 algorithm function f to get $Key_{DH-SHA512}$.



The secret key is $Key = Key_{DH-SHA512}$.

Fig. 2 The procedure of Diffie-Hellman key exchange algorithm with SHA-512

supports privacy homomorphism. Figure 2 provides a procedure of the Diffie-Hellman key exchange algorithm with SHA-512.

4.4 Privacy homomorphism

Privacy homomorphism techniques coined by Rivest et al. [36–38] in 1978 to provide a tool for encrypting the data. The mathematical operations can be applied to the encrypted data even without knowing cover media using privacy homomorphism. The majority of previously published BSWP involves asymmetric key cryptosystem for securing the digital rights of both participants. Our scheme adopts a privacy homomorphism cryptosystem and Diffie-Hellman key exchange to protect the privacy of the participants over the cloud. Privacy homomorphism enables an encrypted environment for the secure transmission of digital content. Eq. (1) represents the privacy homomorphism function.

$$\begin{aligned} P_H &= \mathrm{Enc}^{\mathrm{N}}\left(Key^{\,DH-SHA512}\,(X_1 + X_2)\right) \\ &= \mathrm{Enc}^{\mathrm{N}}\left(Key^{\,DH-SHA512}, X_1\right) \Theta \mathrm{Enc}^{\mathrm{N}}\left(Key^{\,DH-SHA512}, X_2\right) \end{aligned} \tag{1}$$

Where, $\mathrm{Enc}^{\mathrm{N}}$is an encryption function, $\mathrm{Key}_{\mathrm{DH-SHA}}$ is an exchange key between buyer & content owner, X_i is the cover object and Θ homomorphism operator.

4.5 Security in the encrypted domain

This research work provides effective and secure communication between buyer & content owner. Our approach protects the digital rights for both by using the encrypted cloud center

[10]. The encrypted cloud center ensures that the authorized user can access the digital media but he cannot redistribute and leak the media over the internet. Under any circumstance, if the buyer redistributes the content illegally, he can be easily identified by executing watermarking extraction & verifying algorithm.

4.6 Design goals and objectives

The prime objective of this research work is to design a solution to protect the secrecy of the participants involved in purchasing and provide a way against the copy deterrence problem using a semi-trusted third party. The following are the design goals of CB-BSWP.

1. Efficiency. The watermark embedding & signing and watermark detecting & verifying algorithms used in the watermarking process should take less time to execute. These algorithms should achieve a good efficiency for inserting watermarks bits in the media and also extracting from it.
2. Security. The security belongs to the robustness of the watermark, secure communication of the participants and privacy of the data stored in the cloud databases. We adopt fingerprinting-based watermarking to protect digital rights of the content owner and the buyer. In fingerprinting, only the authorized user can decrypt the digital media using the decryption key shared between a buyer and content owner. The suggested CB-BSWP addresses all the issues listed in section 2 required for flexible and secure BSWP.
3. Data privacy. We have used encrypted cloud domains for storing the buyer and content owner's credentials such as watermark, original images, content, watermarked images, digital certificates associated with user IDs. These all entities keep secret on the cloud server for data privacy.
4. Copy deterrence. The content owner should identify illegal copies of the digital media from the authorized user. However, the content owner can frame an innocent buyer by a false allegation and can misuse the buyer's watermark. Therefore, to restrict the content owner the scheme uses a fingerprinting-based method.
5. Watermarking. The watermarking process is shifted to one of the cloud services that is WaaS hence content owner did not know about the embedded watermark into the media. So, the content owner will not be able to frame an innocent buyer. More specifically, the suggested protocol can protect illegal distribution and defend innocent buyer from framing.

5 Proposed CB-BSWP protocol

This section presents the proposed CB-BSWP using a semi-trusted third party for copy deterrence and privacy-preserving. The proposed approach enables the content owner to use the advantages of cloud environments for protecting the digital media before outsourcing to the buyer. Most importantly, we have used two services of cloud: (a) Infrastructure as a service (IaaS) to support virtualized computing infrastructure and ensure the security of the participants by making use of encrypted cloud media (b) Watermarking as a service (WaaS) is used to speed up the process of watermarking that enables the digital content to achieve high efficiency for embedding & extracting the watermarks. The scheme uses CSP to reduce the

burden from (WCA) server, the CSP act as a semi-trusted third party to avoid a situation like WCA becomes unresponsive. CSP reduces the overhead from the trusted third party that is WCA because if the number of users will increase in a network WCA server will become overloaded. The proposed scheme encrypts the digital content by using SHA-512 algorithm with key size 512-bits to ensure that it doesn't affect computational time during the process of encryption. Watermarking as a service (WaaS) for watermarking process and offers a solution for the secure distribution of end-to-end security of digital content over cloud.

The CSP now holds the encrypted digital media on its cloud databases this frees the content owner from not having a separate storage infrastructure. This research work is an extension of our previous research [26, 35]. The content owner should send digital media securely over the internet without compromising the digital rights. The framework of our proposed system model is shown in Fig. 3 and described as follows: (1) the buyer wants to purchase digital media from the content owner. (2) the content owner uses watermark as a service provider (WaaS) for mutual authentication and request for watermark embedding into the digital media and publish it in encrypted form; (3) now buyer apply the decryption algorithm with the public key of CSP, along with shared secret key to obtain the protected digital media. (4) both buyer and content owner have to register with trusted third party TTP that is WCA taking part in a transaction. (5) an ARB is responsible to resolve conflicts between buyer and content owner by executing WEVP algorithm with the assistance of WCA; (6) if suspicious digital media found or produced by spurious buyer the proposed scheme is able to detect the ownership of digital media and can exposes the identity of traitor by detecting the forge watermark $W^{\tau f}$ [39, 40].

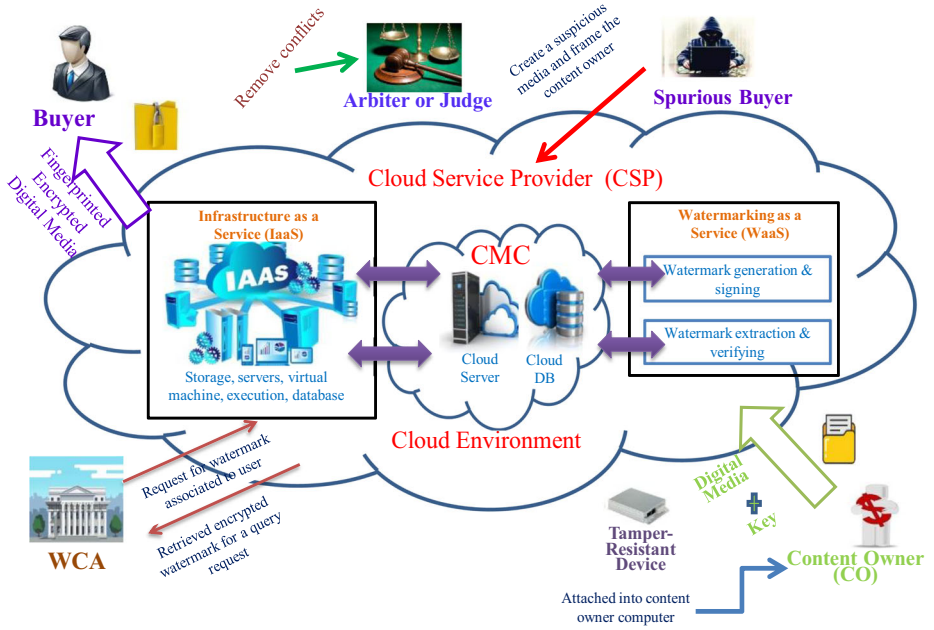


Fig. 3 System model framework of the proposed CB-BSWP

In Fig. 4, the frequency components are selected according to some rules. Adaptive selection of coefficients like DWT coefficients are typically used for dimensionality reduction. The components with high discrimination [32, 33] high accuracy [41] and low correlation [42] should be selected. Figure 4 illustrates the framework for the watermarking scheme in CB-BSWP. This research work is an extension of our previous research [26, 35]. The watermarked images along with watermarks associated with each buyer are stored in the cloud server. In our previous published scheme [26] we have improved Zhang et al. [43] watermarking scheme for gaining high imperceptibility of the watermarked images. The watermark can be extracted by executing the WEVP algorithm and can be compared with the original watermark to identify the ownership of digital media. The CB-BSWP protocol utilizes widely known security provision: robust and fair watermarking scheme, privacy homomorphism [36–38] for implementation. The fair watermarking scheme, hold up blind detection of watermarks, these embedded watermarks can resist against modifications and image processing attacks. If a forge and suspicious digital media is found it can be easily detected by using fair watermarking scheme. The use of a cloud environment restricts the partial involvement of both the participants in the process of generating the encrypted watermark. Therefore, no one can frame each other. This reduces the requirement of a TTP, leads in more secure and practical economic cloud-based BSWP. For the watermarking process frequency components are selected based on low frequency coefficients because it contains less information of the image which results in less impact in the watermarking process. DWT low frequency coefficients are used for selection and dimensionality reduction of the frequency components in fig. 4. The components with high discrimination contains most of the image information leads in low imperceptibility. The watermarking scheme used in the protocol involves a secret key generated by Diffie-Hellman key exchange followed by secure has algorithm (SHA-512) for secure communication [44].

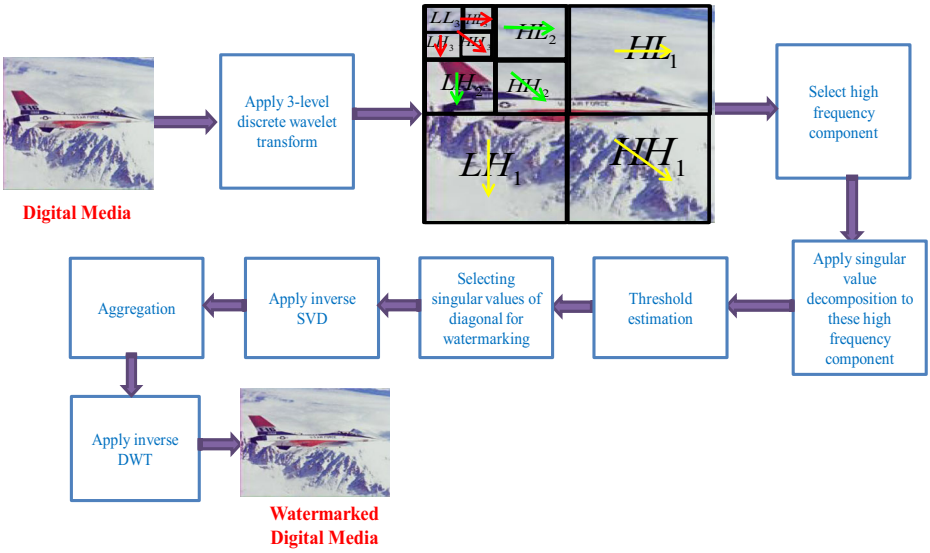


Fig. 4 Framework for the watermarking scheme in CB-BSWP [32, 33, 35]

The cloud server stores the digital media, watermarks, watermarked media, secret keys, certificates of involving participants, IDs of each participant, public keys and digital signature in encrypted form using cloud media center that allows only authorized users can access the cloud server.

Our proposed scheme considered some assumptions to design CB-BSWP that uses a cloud environment efficiently. These assumptions are listed here.

1) All the transactions should use timestamp, nonce and unique watermark for digital media.
2) The CSP acts as a trusted signatory, and should not exploit their role.
3) The digital media is still an image in the suggested protocol.
4) The public key cryptography and the fingerprinting scheme should be very inconvenient to use for the adversary.

These assumptions assist the proposed CB-BSWP to use the advantages of a cloud environment for setting an encrypted domain to store secret data in real-time implementation. Following are the goals for proposed CB-BSWP protocol described below:-

1) Watermark generation, insertion and verifying phase use a robust fingerprinting scheme. Our protocol uses watermarking as a service to support the speedy process of watermarking. By inserting a unique watermark into the digital media, the CB-BSWP protocol can control illegal copy.
2) Provide an encrypted environment for storing sensitive information to preserve the privacy of the participants. The scheme reduces the overhead from the watermarking certificate authority (WCA) by using a cloud service provider. The buyer can be anonymous during the purchasing of digital media in a transaction.

We have defined the roles and descriptions of various participants of the proposed approach as shown in Fig. 3.

- Buyer (B): Customer who wants to purchase digital media DM from the content owner CO generally the buyer B is considered as a consumer of digital media.
- Content Owner (CO): Image owner or seller who posseses digital media. The content owner CO has digital media and wants to securely transmit it to the buyer using cloud environment CE. The use of encrypted cloud protects the data from unauthorized access and security breaches.
- Arbiter (ARB): An arbiter checks for authenticity of digital media DM and solves the conflicts between the communicating participants. ARB is known as a judge by communicating with trusted third party ARB solves the problem of piracy tracing and copyright infringement.
- Watermark Certificate authority (WCA): It is a trusted third party TTP responsible to generate watermarks for the CO once received authorized request from CO. WCA generates digital signature DS for a transaction. We have used watermarking as a service to reduce the overhead from the WCA. It operates as a group manager, responsible for signing and issuing the validity of the anonymous certificates before a transaction.
- Cloud media center (CMC): Cloud media center CMC ensures that only authorized users can access the resources from the cloud. CMC is responsible for storing the encrypted DM

in the cloud database. Once, DM is requested by CO, it acts as a delegate model for an authorized user to provide the service.

- Tamper-resistant device (TRD): It is used to protect the privacy of user sensitive data from unauthorized use and reduces the overhead from the TTP. This device is attached to the content owner system to reduce the overhead and utilize the cloud environment CE for storage.
- Cloud service provider (CSP): It is considered as a "semi-trusted" third party and it provides a platform for executing infrastructure and storage services on the cloud. CSP monitors data in cloud servers, CS protects the data stored in the cloud by using encrypted cloud media center CMC.
- Cloud server (CS): A cloud server CS is a virtual machine responsible for hosting and delivering the application on a cloud computing platform via network and can be accessed remotely. These virtual machines have installed software required to run as independent units and store all encrypted digital media along with the key.
- Spurious buyer (S_P): Who pretends to be a legitimate buyer, but is instead a fake user and claims for digital media that does not belong to him.

The general process of watermarking takes place as follows: to embed the watermark W into the digital media DM where XDM is a watermarked digital media [9].

$$DM = (DM_1, DM_2, DM_3, \ldots . DM_n) \tag{2}$$

$$W = W_1, W_2, W_3, \ldots\ldots\ldots\ldots .W_n\Big) \tag{3}$$

The scheme can be represented as the computation of

$$XDM = \{W_1 \otimes DM_1, W_2 \otimes DM_2, W_3 \otimes DM_3, \ldots\ldots\ldots\ldots .W_n \otimes DM_n, W_{n+1} \otimes DM_{n+1}\} \tag{4}$$

Where ⊗ represent watermarking embedding algorithm. Furthermore, the encrypted digital media can be represented as follows. The Eq. (2) to the Eq. (5) shows the watermarking system.

$$Enc^N{}_{pk}(XDM) = Enc^N{}_{pk}\{W_1 \otimes DM_1, W_2 \otimes DM_2, W_3 \otimes DM_3, \ldots .. \ W_n \otimes DM_n, W_{n+1} \otimes DM_{n+1}\} \tag{5}$$

The encryption system $Enc^N$is considered as privacy homomorphism for the watermarking process ⊗ in a secure environment. The proposed CB-BSWP protocol consists of three phases: registration phase, the watermark generation & signing phase WGSP, and watermark extraction & verifying phase WEVP as shown in Fig. 5. The registration phase shows an interaction between Buyer B and certificate authority CA; content owner CO and CA; CA and CSP. The key-exchange protocol is performed among B, CA and CO for secure transmitted of secret keys in encrypted form with a digital certificate. In any case, if conflict arrives between B and CO, it is a responsibility of ARB to resolve that issue by using his private key to decrypt the

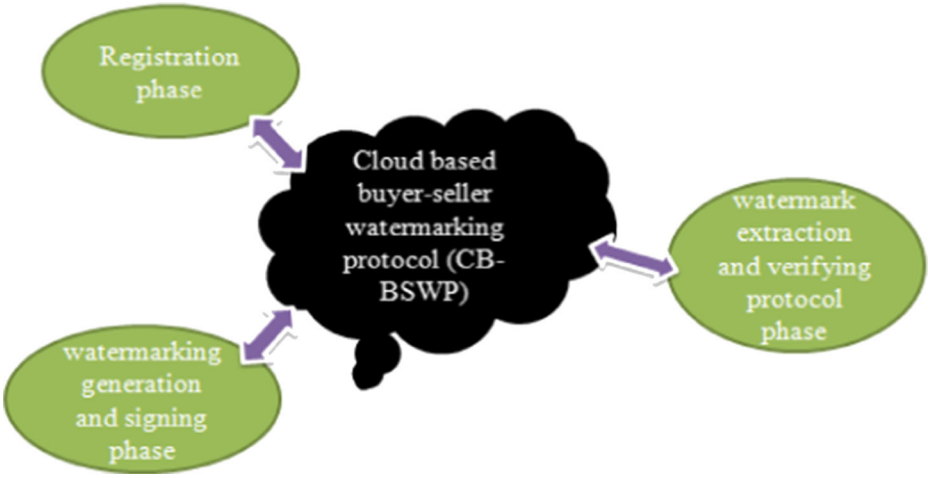


Fig. 5 Cloud based buyer-seller watermarking protocol (CB-BSWP) phases

watermarked digital media XDM and identify the true owner digital media. The WGSP phase is carried out between CO and CSP. The WEVP phase is executed between ARB, CSPand CA to identify the suspicious SDM and S_P spurious buyer.

5.1 Registration phase

In the registration phase, content owner CO and buyer B have to register themselves respectively, with a certificate authority CA before the transaction T^N starts. In our scheme, only buyer B has to communicate with the certificate authority CA once at the time of registration. The messages M_i transferred between the buyer B and certificate authority CA in an encrypted domain E^N are free from tampering. If buyer B does not want to expose his identity ID_B an anonymous digital certification $UCert_B$ will be issued to the buyer B. In the registration phase, buyer B can choose a digital media DM and purchased it from the content owner CO in a transaction. To start the negotiation, buyer B selects a random key pair of key (PRU_B, PKR_B) and sends PKR_B to a certificate authority CA. After receiving the request certificate authority CA generates an anonymous digital certificate $D_{SUCertB}$ $=E(PR_{CA}(ID_{CP},t,X,W,DM))$ and sends it to the buyer B. The following steps are performed during the registration phase.

Step 1: If buyer B wants to communicate with the content owner CO he initiates a request message M to the CA requesting an anonymous certificate $UCert_B$ so that he can start communicating with CO. Certification authority first checks the identity ID_B of the buyer and checks the creditability of CO.

Step 2: After step 1, if all credentials is valid CA generates an anonymous certificate DS_{UCert} and issues it to buyer B.

In the registration phase, the interaction between buyer B and certificate authority CA is depicted in Fig. 6. This interaction allows B for purchasing a DM from the content owner CO in a transaction. First B initiates a request to the CA demanding the identity ID_{CO} and public

Buyer B	Certificate Authority CA
$B \rightarrow$	: Buyer who wants to purchase a DM from content owner CO
$B \rightarrow CA$	: $M1=\{Request// ID_{CO} // Cert_B\}$
$CA \rightarrow B$	: $Enc^N\{PR_{CA}(ID_{CO}, t_1, N, W, PU_{B,} Cert_B)\}$
$B \rightarrow CO$	: $M2=\{N_2// ID_{CO} // Cert_B\}$
$CO \rightarrow B$	: $Enc^N[PR_{CO}(ID_{CO}, t_2, N, W, PU_{CO,} Cert_{CO})]$
$B \rightarrow CO$	: $M3=\{Request\ for\ Digital\ Media\ DM\}$
$CA \rightarrow$	: $Key_{DH\text{-}SHA512}(Sk_{CA}), (Rpk_B, Rsk_B)\ N,\ Enc^N{}_{PR_B}(Enc^N{}_{PR_{CA}}(DM))$
$CA \rightarrow B$	: $M4=\{ID_{DM}, Sk_B\}$
$CA \rightarrow CO$	: $M5=\{ID_{DM}, Pk_B, PU_{CO,} Sk_{CO}, E_{PR_{CA}}, E_{PR_{CA}}(DM)\}$
$CA \rightarrow B$	: $DS_{UCert_B} = E(PR_{CA}(ID_{CP}, t, X, W, DM))$

Fig. 6 The registration phase between buyer and certificate authority

key PU_{CO} of the content owner CO. In one-time interaction total, 5 messages M is transferred, once B gets a response from the CA then B sends a request to CO for DM. CA verifies the credentials of B and issues a digital signature DS signed by its own private key PR_{CA} sent to B, with this digital signature DS, B can interact and purchase DM form the CO.

5.2 Watermark generation and signing phase (WGSP)

In the watermarking generation and signing phase (WGSP) the watermark W is generated by the content owner CO along with cloud service provider CSP for the digital media DM into a transaction. This process is executed multiple times among the content owner CO, watermark certificate authority WCA and cloud service provider CSP. The content owner CO uses WaaS service from the cloud environment CE and the communication is performed using CSP. Buyer B verifies the received digital media XDM sent from the content owner CO to check the purchasing record with the help of nonce N value. For that, buyer B generates a key pair (PU_B, PR_B), timestamp T, identity ID_B and other information for the transaction sends this to the content owner CO after encrypting with buyer's B private key PR_B. The content owner CO wants to send the encrypted digital media DM then the CO carried out watermarking generation & signing protocol (WGSP) with WCA and cloud service provider, CSP as shown in Fig. 7.

5.3 Watermark extraction and verifying phase (WEVP)

This phase is executed for checking the integrity of digital media DM, identification of spurious buyer S_P,and to expose the identity of the traitor. This protocol is carried out among arbiter ARB, CO, B, CSP and WCA. This protocol is executed when a suspicious digital media SDM is found in a protected covering object and to identify the spurious buyer S_P who is responsible for the distribution of illegal digital media DM. If the arbiter (judge) receives a SDM then CO can claim the legitimate copyright ownership by running the watermark extraction and verifying phase WEVP. The content owner CO wants to prove the ownership

Input: Cover object X, Timestamp T, identity ID_{CO}, digital media DM, Nonce N
Output: CO generates W^{CO} and Key, WCA obtains W_{CSP}^{WCA}
Procedure: Generation & Embedding
Step 1) The content owner CO select a random watermark W.

1. $Select \leftarrow WatRan\ (W)$
2. $W \leftarrow WatGen^{algo}\ (X, W, Key)$
3. $W^{\tau} \leftarrow E_{PR(CO)}(W)$

Step 2) The CO inserts the encrypted random watermark W into DM to obtain watermarked data XDM.

1. $XDM \leftarrow E_{PR(CO)}(W^{\tau}, DM, T, ID_{CO}, Pk_{CO})$
2. $SecEmb \leftarrow$ Watermark into DM
3. $Enc^{N}PR_{CO}(W^{\tau}) \leftarrow Enc^{N}(PR_{CO}, W^{\tau})$

Step 3) Then CO obtain XDM and perform the public-key cryptosystem PC_{WCA}.

1. $Enc^{N}(XDM)PC_{WCA} \leftarrow E_{PR(CO)}(W^{\tau}, DM, T, ID_{CO}, Pk_{CO})$

Step 4) The CO store and send the generated random encrypted watermark to the cloud.

1. $Store_{Pkco} \leftarrow T, Enc^{N}(PR_{CO}, W^{\tau})$ and send one copy to WCA
2. $Send^{pkco} \leftarrow Enc^{N}(XDM)PC_{WCA}$ and $Enc^{N}PR_{CO}(W^{\tau})$ to the cloud

Step 5) Now WCA generates its own watermark W apply encryption with private key Psk_{WCA}.

1. $W^{wca} \leftarrow WatGen^{algo}\ (X, W, Key)$
2. $Enc^{N}(W^{wca})PC_{WCA} \leftarrow Enc^{N}(Psk_{WCA}, W^{wca})$
3. $Send^{Pskwca} \leftarrow Enc^{N}(W^{wca})PC_{WCA}$ to the cloud

Step 6) Cloud service provider CSP received both encrypted watermark W^{wca}, W^{τ} for the XDM perform.

1. $Enc^{N}(W^{\tau}, W^{wca})PRk_{CSP} \leftarrow Enc^{N}(XDM, PRk_{CSP})$
2. $Send\ Enc^{N}(XDM)$ to the content owner CO
3. $Sign_{PRkCSP} \leftarrow Enc^{N}(XDM)$

Step 7) CSP keeps a record of the entire transaction including, timestamp, watermark, digital media, the identity of the participants into the cloud server CS. Now, CO can publicize the XDM to the B.

1. $Store \leftarrow (XDM, ID_{user}, N, T, W)$ into the CS.

Fig. 7 The watermarking generation and signing phase in (CB-BSWP)

of a digital media DM and identify the traitor then the CO carried out this phase with WCA, a cloud service provider as shown in Fig. 8.

5.4 Infrastructure as a service (IaaS)

Two services of cloud computing provide a supporting infrastructure to design a proposed CB-BSWP that can utilize a cloud computing platforms to protect the participant's security and support the watermarking process as well in a "semi-trusted" cloud computing environment. Infrastructure as a service (IaaS) to support virtualized computing infrastructure and ensure the security of the participants by making use of encrypted cloud media where multiple virtual machines are running. In this service, CSP launches the required infrastructure, storage, servers, virtual machine, execution, database and network support hardware. The content owner can use this secure and effective infrastructure provided over the internet by CSP on the basis of monthly or yearly charges. Therefore, the content owner can save its expenses incurred in maintaining hardware and network devices separately on the client side. Now, the content owner has to pay expenses based on pay to use model which results in money saving and the buyer can access the resources from anywhere and anytime through the internet connection.

Input: Watermarked digital media XDM, Timestamp T, watermarked cover object X^{τ}, Nonce N'
Output: User's Identity ID and Recovered watermark
Procedure: Extraction & Verifying
Step 1)The content owner CO sends both embedded watermark W^{τ}, W^{wca} along with suspicious digital media SDM to the Arbiter ARB.

1. $Send \rightarrow W^{\tau}, W^{wca}\ and\ SDM$

Step 2) Then ARB performs the decryption of every element Dec^{N} with a private key to obtain $Dec^{N}(W^{\tau}, W^{wca})$ from the watermarked digital media XDM.

1. $ARB \rightarrow Dec^{N}(W^{\tau}, W^{wca})PRk_{ARB}$ and SDM
2. $W^{\tau\prime} \leftarrow WatDet^{\,algo}\,(XDM, W^{\tau}, Key)$
3. $W^{wca\prime} \leftarrow WatDet^{\,algo}\,(XDM, W^{wca}, Key)$

Step 3) Now arbiter ARB sends both extracted watermark $W^{\tau\prime}, W^{wca\prime}$ to cloud service provider CSP for the decryption.

1. Send$\rightarrow Dec^{N}(W^{\tau}, W^{wca}), XDM, PRk_{CSP}))$
2. $Compare \rightarrow ((W^{\tau}, W^{wca}) == (W^{\tau\prime}, W^{wca\prime}))$

Step 4) Cloud service provider CSP can identify spurious buyer S_P associated with XDM by executing $WEVP$ using $Dec^{N}(XDM, PRk_{CSP})$.

1. $CSP \rightarrow (XDM, PRk_{CSP})$

Step 5)The arbiter ARB verifies the correctness of elements sent from CSP using sign verification algorithm and exposes the identity of the traitor.

1. $VerNSign \leftarrow Dec^{N}(DM, PRk_{CSP})$
2. $ID_{S_P} \rightarrow (DM == SDM))$

Fig. 8 The watermark extraction and verifying phase in (CB-BSWP)

5.5 Watermarking as a service (WaaS)

Watermarking as a service WaaS is used to speed up the process of watermarking that enables the digital media to achieve high efficiency for embedding & extracting the watermarks. The watermarked images along with watermarks associated with each buyer are sent to the cloud environment for further processing [6]. This relieves the burden from the WCA for storing watermarked content and enables our scheme to have a "semi trusted" third party in the cloud computing environment. These watermarks can be recovered from the watermarked color images and compared to the original watermark for identifying the owner of the digital media. The buyer checks the correctness of obtained digital media and can analyze the purchasing record with help of nonce value. WaaS service is responsible for the watermark generation & signing phase and watermark extraction & verifying phase in a semi-trusted cloud computing environment.

6 Solution analysis of proposed CB-BSWP

In this section, the efficiency and effectiveness of the proposed CB-BSWP are evaluated concerning the parameters shown in Fig. 1. The safety of the proposed CB-BSWP protocol depends on the watermarking embedding and extraction algorithm. The proposed approach relies upon, the security of the cloud environment and requirements of flexible & secure

BSWP scheme. The watermarking embedding and extraction algorithm is based on the following assumptions. First, these algorithms must be robust against the attacks, and the embedded watermark should be robust against attacks [45–47]. However, in the literature, we found that no such watermarking scheme exists with good robustness and imperceptibility. Second, the public key infrastructure PKI along with a key exchange algorithm should ensure that an attacker in any case will not be able to get knowledge of digital media, secret key and the embedded watermark. Lastly, the solution must use privacy homomorphism cryptosystem to make impractical for an adversary to carry out security related attack [48]. Our proposed CB-BSWP protocol gives a solution to the privacy-preserving and copy deterrence so first, we analyzed the security of participants.

6.1 The buyer security

Privacy homomorphism P_H cryptosystem with key exchange algorithm $Key_{DH\ -\ SHA512}$ is the important components of CB-BSWP to enable digital media DM and secret key *ks* to be securely transmitted. Even though if an unauthorized buyer S_P gets access to watermarked digital media XDM, still he will not be able to carry out the attacks and modify the secure data. More specifically, to protect the innocent buyer B, a unique watermark W is embedded in the digital media DM using WaaS cloud service, so that content owner CO could not frame the buyer B. The embedding of the watermark is done in such way, that CO does not know the presence of watermark bits into DM, therefore, CO cannot frame the buyer B. On the other side when the buyer B obtained the watermarked digital media XDM from the CSP by providing his unique certificate $Cert_B$, still he would not detect the exact location of the watermark W bits presented in digital media DM. To handle conflicts between content owner CO and buyer B, the ARB provides the actual watermark W and watermarked cover object X^{τ} by communicating with watermark certificate authority WCA to resolve the dispute [49]. To control copy deterrence, watermark W is embedded by the WCA making use of CSP, content owner CO and buyer B has partial involvement of the watermarking process therefore it is impractical for a buyer B to frame the content owner CO.

1. $W^{wca} \leftarrow WatGen^{algo}(X, W, Key)$

2. $W^{\tau} \leftarrow E_{PR(\ CO)}(W)$

6.2 The content owner security

Content owner CO security is very important in the CB-BSWP because CO needs cloud media center CMC to provide an encrypted environment to manage the secure interaction between CO and B buyers with a semi-trusted third party. CO makes use of cloud computing services such as WaaS to support the protection of watermarks into the digital media DM and IaaS to provide a way for storing the secret credentials of the participants through a storage infrastructure. If the B wants to cheat with CO by producing a forge watermark $W^{\tau f}$ and suspicious digital media SDM. Then, CO produces a nonce N value along with a timestamp identifier for a particular transaction with the buyer B, compares the transaction details with the claiming buyer B can directly identify spurious buyer S_P and exposes the identity of the traitor.

1. $VerNSign \leftarrow Dec^{N}(DM, Prk_{CSP})$

2. $ID_{S_P} \rightarrow (DM == SDM)\Big)$

6.3 Efficiency

This section presents the efficiency of watermarking generation & signing algorithm; and watermark extraction & verifying algorithm. The efficiency directly relies on the privacy homomorphism P_H cryptosystem, to provide an encrypted domain for WaaS cloud service to embed encrypted watermarks directly into digital media DMbefore sending it to the content owner [50]. We analyze the significant computational costs of these two algorithms in terms of computation, communication, and storage. Let suppose two buyers B makes a request of digital media DMto CO simultaneously, then the computational complexity depends on the privacy homomorphism operations for inserting of buyer's watermarks. This complexity directly relies on the encryption process of CO watermarks which is embedded with the assistance of cloud service provider CSP into the digital media DM.In our scheme, the cloud environment has infinite computational power and storage capacity as an assumption. Therefore, we can ignore the time and storage complexity in efficiency analysis. When a spurious buyer S_P tries to frame innocent CO, S_P has to produce suspicious digital media SDM, forge watermark $W^{\tau f}$ to the ARB and make an allegation to innocent CO. However, in our scheme buyer B does not have any knowledge where exactly the watermark bits are inserted into digital media DM.Hence, it is impractical for spurious buyer S_P to frame an innocent CO because the watermarking algorithm is secure enough.

6.4 Security

The suggested CB-BSWP allows partial involvement of buyer B, content owner CO during the process of watermarking into the digital media DM that ensures the security of the watermark. Privacy homomorphism cryptosystem and Diffie-Hellman key exchange is used to protect the privacy of the participants over the cloud. The cloud service provider CSP performs encryption by its private key PRk_{CSP} on $(XDM, W^{\tau}, DM, T, ID, Pk_{CO})$ and makes a copy of the encrypted data on cloud server CS and records it. Therefore, it is impossible to break the security of encrypted data on the cloud, and creating a copy of the encrypted data before outsourcing is very much essential to resolve the conflicts.

6.5 Flexible and secure watermarking

The performance of the proposed CB-BSWP protocol against the requirements mentioned in section 2 is shown in this section.

- Anonymity problem: The proposed CB-BSWP provides a provision that if a buyer B does not want to expose his identity, an anonymous digital certification $UCert_B$ will be issued to the buyer B by sending this anonymous digital certification he can interact with WCA and CO. The suggested protocol did not reveal the identity of B until a suspicious digital media DM is found. Therefore, privacy is preserved for buyers and anonymity is maintained using a cloud environment.

The scheme randomly generates a pair of keys (PR_B, PU_B) to protect the buyer's identity for the transaction.

$$DS_{UCert} = E(PR_{CA}(ID, t, X, W, DM))$$

- Tamper Detection: The content owner's computer is attached with a tamper detection device to detect the modifications to digital media DM by a spurious buyer S_P and reduces the overhead from the TTP. In any case, the adversary should not be able to gain the knowledge of inserting watermarks bits.
- Non-framing: Content owner CO cannot construct a buyer for unlawful redistribution of digital media DM because the buyer can claim that the digital media does not belong to him by sending all required details to the arbiter ARB that act as Judge. In such cases, ARB will execute the watermark extraction & verifying algorithm to identify the guilty one. Therefore, the watermarking system does not allow for a false allegation of an innocent buyer.
- Non-repudiation: The algorithms used in CB-BSWP contains (1) timestamp T for recording the interaction time between buyer B and content owner CO; (2) nonce N value of the uniquely identified transaction. Hence, both the participants cannot deny a transaction if they are involved. Content owner CO and watermark certificate authority WCA watermarks (W^{τ}, W^{wca}) are registered with CSP which contains the identity of both.
- Customer's rights problem: The CB-BSWP keeps the buyer's watermark W secret, which prevents a content owner CO from misuse the buyer's B watermark W because the process of watermarking is done by CSP without revealing the buyer's watermark W to the content owner CO. Therefore, if CO wants to redistribute buyer's watermark W into other digital media CO will be easily identified.
- Traceability: In our proposed approach, we have used a semi-trusted third party as CSP to reduce the burden from WCA for storing encrypted data. Privacy homomorphism cryptosystem P_H is used to make sure that digital media obtained by buyer B have the CO ' s watermark encrypted by cloud service provider CSP. Watermark extraction & verification WEVP algorithm can identify the pirated copy of digital media.
- Privacy preserving: Our scheme maintains the privacy-preserving property because the scheme adopts privacy homomorphism cryptosystem P_H and Diffie-Hellman key exchange to protect the privacy of the participants over the cloud. Cloud media center ensures that the cloud data cannot be altered or viewed by an unauthorized user and it should be stored in cloud server in an encrypted form. These two together create an encrypted domain environment for the secure exchange of data between buyer and content owner hence privacy is preserved.

6.6 Comparisons

In this section, we have compared our proposed CB-BSWP using a "semi-trusted" third party to the previous published protocol as shown in Table 2. In Table 2, we have shown a detailed comparison of CB-BSWP protocol with previously published BSWP's solutions [26, 35, 40, 43, 51–56]. We have tested the performance of CB-BSWP with the problems listed in section 2. Table 2 illustrates the performance comparison of the proposed CB-BSWP. The properties used to ensure the security of the participant over the cloud are value-added services, power

Table 2 Comparison of CB-BSWP with previous published BSWP [26, 35, 40, 43, 51–56]

S. N.	Author's Name	Encryption Scheme	Digital Media	Type of Watermarking	System Model	Security Problems Solved in BSWP					
						AP	NFP	NRP	CRP	TP	UP
1	Ferrer and Megias [52]	Asymmetric Encryption	Audio	Robust Double Watermarking	Trusted Registration Party	yes	yes	yes	___	no	__
2	Frattolillo [40]	Asymmetric homomorphic encryption	___	Robust Watermarking Scheme	ONWA	yes	no	yes	no	yes	yes
3	Eslami and Kazemnasabhaji [53]	Proxy Signature	Image	Robust	No TTP	yes	___	yes	no	yes	yes
4	Yu et al. [56]	Not specified	Software	Robust	Trusted Cloud Watermarking	no	yes	yes	yes	yes	no
5	Chang et al. [51]	Hybrid	___	Not Specified	Requires a Trusted (WCA)	yes	yes	___	yes	yes	no
6	Ashwani Kumar [35]	Not specified	Images	Robust DWT	Zero-knowledge proof	no	yes	yes	no	__	___
7	Jianquan and Qing [55]	Asymmetric Encryption	Images	Robust Watermarking	No third party involvement	no	yes	yes	yes	yes	no
8	Zhang et al. [43]	Asymmetric homomorphic w.r.t addition	___	Spread Spectrum DCT	Zero-Knowledge Proof, No TTP	__	yes	yes	no	yes	___
9	Shao et al. [54]	Asymmetric RSA Homomorphic	___	___	Semi trusted third party	yes	yes	yes	no	no	___
10	Ashwani Kumar [26]	Asymmetric encryption	___	DWT	Trusted WCA is required	no	___	yes	no	yes	yes
11	**Proposed CB-BSWP**	**Asymmetric Privacy Homomorphism**	**Image**	**Robust and Invisible watermarking scheme**	**Semi-Trusted Third Party with Cloud Environment**	**yes**	**yes**	**yes**	**yes**	**yes**	**yes**

Table 3 Cloud computing services used for ensuring cloud security

Cloud Services Parameters	IaaS with Cloud Computing	WaaS with Cloud Computing	Physical Server
Response to buyer B request	Automatic process and Fast	Cooperate with WCA to support the watermark process at the cloud	Manual action is performed and slow.
Power consumption	Reduce power by server consolidation and sharing	Scheduled power off needed for could server CS	Normal
Storage consumption	Virtual Machine and cloud server CS is Used	Virtual machine and cloud database CD are used	Depends on the capacity of sever
Value add service	Rich and storing the secret credentials in the encrypted domain	Ubiquitous access to resources End to end request management	Very few
Mode of operation	Automatic and integrated operation	Integrated operation	Manual operation
Authentication and authorization	Virtual machine authentication	CSP authentication	Firewall software needed

Table 4 Watermarked images used for experiment

Total Watermarked Images	1000	1500	2000	2500	3000	3500	4000
CB-BSWP in Cloud Environment	78	209	**328**	**250**	**480**	**690**	805
Client Side Local Computer	140	151	200	218	300	327	367

consumption, storage consumption, response time, operations and authentication services [18]. The content owner CO takes the advantages of value-added services with a quick response time in cloud computing environment as shown in Table 3.

6.7 Complexity analysis

The complexity of proposed CB-BSWP protocol is analyzed in this section. Table 4 shows the different values for the watermarked images when executed on cloud environment and local personal computer. It clearly shows that when cloud environment is used these watermarked images achieve good performance as compared to local machine.

The proposed approach relies upon, the security of the cloud environment and requirements of flexible & secure BSWP scheme. Figure 9 demonstrates the number of watermarked images increases linearly with correspond to time as the interaction increases between buyer and seller.

7 Performance analysis of CB-BSWP

Simulation results to calculate the performance of watermarking insertion and extraction algorithm against image processing attacks are shown in this section. The CB-BSWP is enforced in MATLAB 2018a environment on a dell studio PC, Intel (R) Core (TM) 2 Duo

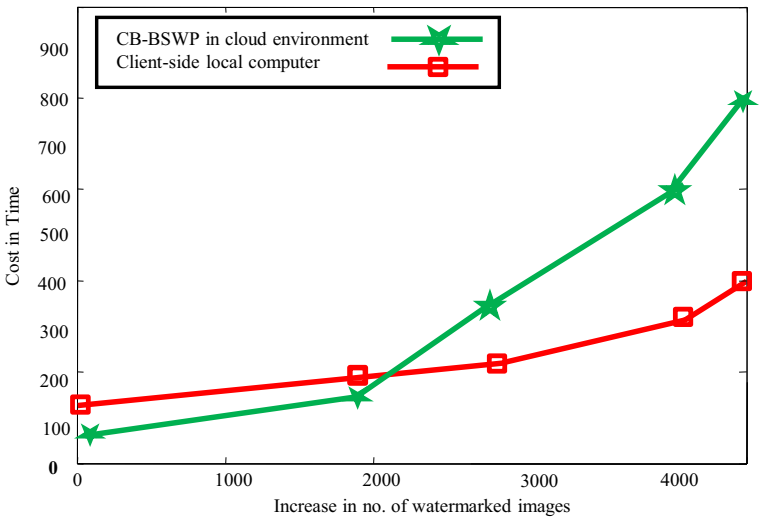


Fig. 9 Demonstrates the number of watermarked images

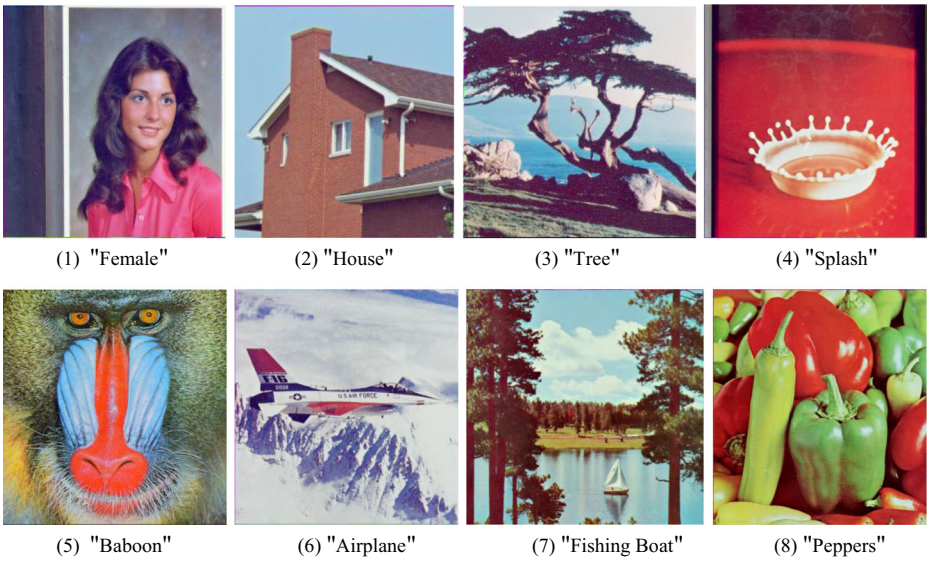


Fig. 10 Eight sample images taken with size of 512 × 512 pixels for conducting experiments

CPU T6600 @ 2.20 GHz and 4.00 GB RAM. The colored images are taken from the database of the standard images for conducting this research work. The database is available http://sipi.usc.edu/database in this URL [57]. The existing BSWP uses Cox [58] method to gain robust watermarking. We adopt a fair watermarking scheme with privacy homomorphism cryptography to achieve great robustness in watermarks and ensure high imperceptibility for the watermarked images. We have used eight sample color images with a size of 512 × 512 and 4 grayscale watermarks of size 64 × 64 as demonstrated in Fig. 10 and Fig. 11 for the watermarking process. These watermarks are embedded into these color images using the watermark generation & signing phase (WGSP) discussed in sub-section 4.2. The inserted watermarks can be extracted from the digital media by executing watermark extraction & verification phase (WEVP) as presented in sub-section 4.3. For checking the quality of watermarked images peak signal-to-noise ratio (PSNR) is commonly applied. Therefore, we used (PSNR) to evaluate the perceptual quality of color images and mean square error (MSE) to find out error between the watermarked digital media XDM and original digital media DM for accuracy. The less value for MSE indicates the greater robustness of the watermark.

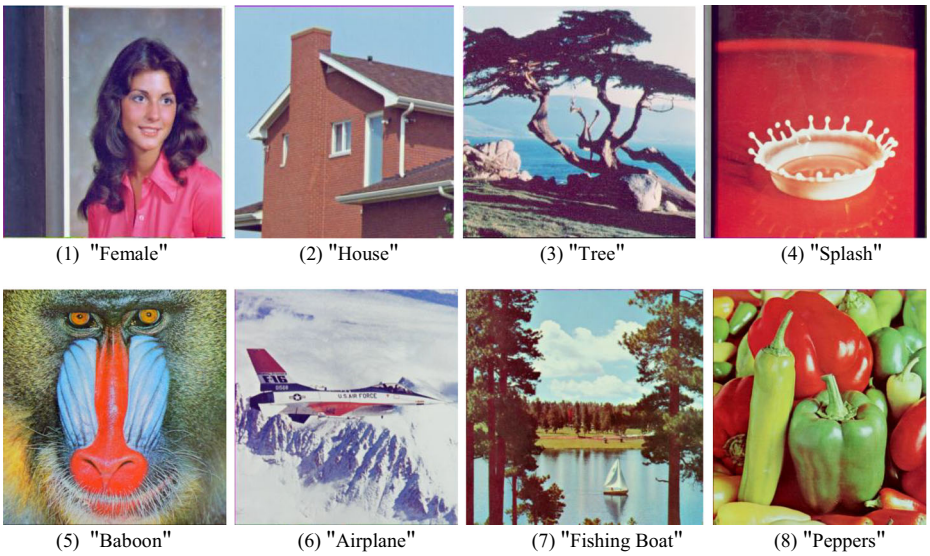
Fig. 11 Grayscale watermark images of size 64 × 64 (a)"College logo"(b)"Watermark"(c)"Digital media"(d) "Diamond"

Table 5 PSNR (in dB) results for sample color watermarked images and original images

	Original PSNR	Salt & pepper noise with different density				Speckle noise with different density			
		μ=0.02	μ=0.04	μ=0.06	μ=0.08	μ=0.02	μ=0.04	μ=0.06	μ=0.08
"Female"	48.32	47.95	46.58	45.61	43.85	47.35	46.15	45.56	44.49
"House"	47.57	46.67	45.09	44.35	42.16	45.81	44.01	43.63	42.88
"Tree"	46.81	44.23	43.76	42.65	41.53	45.32	44.54	43.77	41.20
"Splash"	51.97	50.96	48.91	47.23	45.37	49.23	48.46	47.23	45.36
"Baboon"	45.93	43.62	42.33	41.89	40.86	44.06	43.91	42.16	40.39
"Airplane"	51.01	49.41	48.67	47.41	45.42	50.73	49.12	47.87	46.56
"Boat"	46.65	44.12	43.43	41.87	40.07	45.04	44.86	43.89	42.74
"Peppers"	48.06	47.73	46.42	45.23	44.90	46.93	44.35	42.66	41.90

Table 5 highlights the PSNR values of the colored watermarked images shown in Fig. 12. We have applied salt & pepper noise with different range $\mu = 0.02$ to $\mu = 0.08$, speckle noise with a range from $\mu = 0.02$ to $\mu = 0.08$ for all eight watermarked images and tested the performance, the corresponding PSNR values are given in Table 5. It is observed that the proposed scheme is suitable for fair watermarking against salt & pepper noise because the PSNR values reach above 44 dB for some color images like "Splash", "Airplane" and "Peppers" which is highly appreciable for image processing applications.

The watermarks "college logo", "watermark","digital media" and "diamond" are embedded into the sample images for checking the robustness of the watermarks. For this purpose, known image processing attacks are applied to these sample images as given in Table 5. Furthermore, the integrated watermarks can be recovered from the attacked sample images using the watermark extraction & verification phase (WEVP) as represented in subsection 4.3. Figure 13 and Fig. 14 represent the extracted watermark "College logo", "Watermark", "Digital media"



(1) "Female" (2) "House" (3) "Tree" (4) "Splash"

(5) "Baboon" (6) "Airplane" (7) "Fishing Boat" (8) "Peppers"

Fig. 12 Watermarked color images with size of 512 × 512 pixels

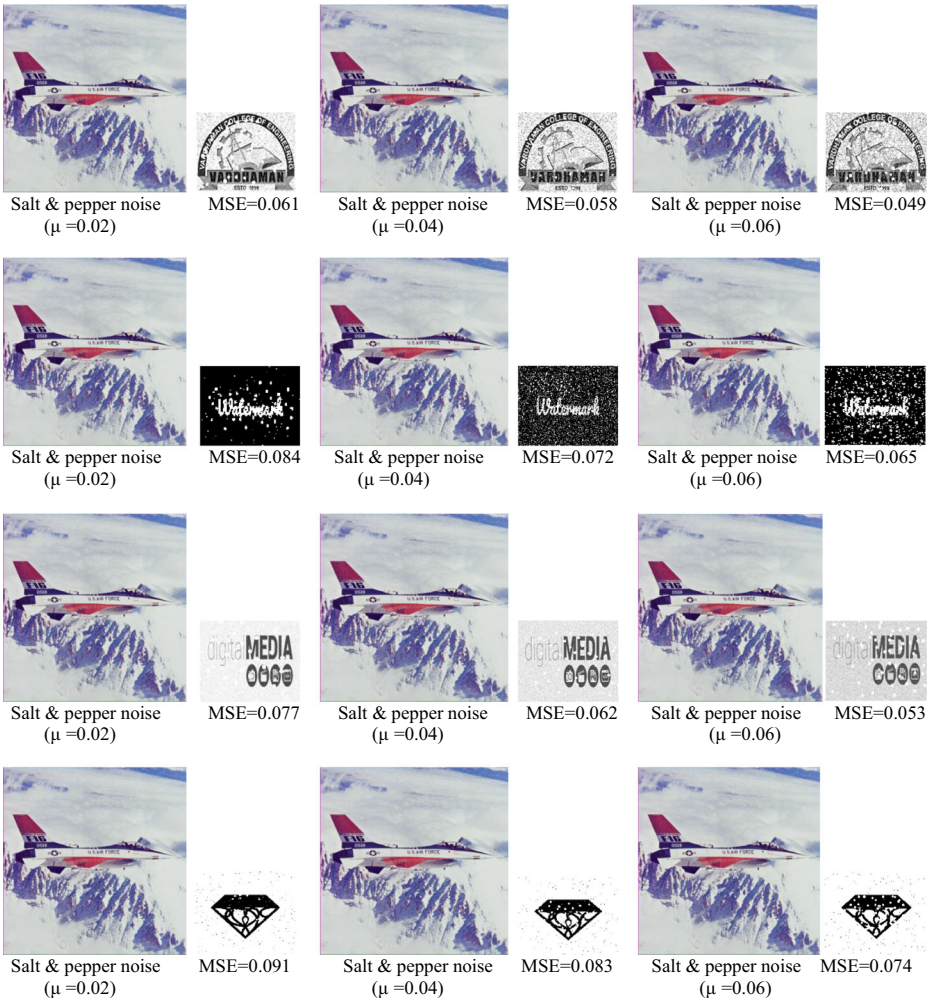


Fig. 13 Extracted watermarks "College logo", "Watermark", "Digital media" and "Diamond" from the attacked "Airplane" images against salt & pepper noise

and "Diamond" from the attacked sample images of "Airplane" and "Tree" respectively. The scheme performs well in the case of speckle noise for robust watermarking because the PSNR values reach above 45 dB for some color images like "Splash" and "Airplane" which is well accepted. Figure 12 shows the perceptual quality of watermarked color images, these images contain high resolution, even though the watermark is present in the images, hence high imperceptibility is achieved.

Figures 15 and 16 show the PSNR values of watermarked images obtained from the CB-BSWP protocol by applying attacks such as salt & pepper noise and speckle noise. These graphs show the relationship between the watermarked image and the noise. We have used μ to represent the noise density. As the amount of noise increases the values of PSNR decreases, but still, no big perceptual degradation is found and resistance power to sustain the content owner watermark is strong as well.

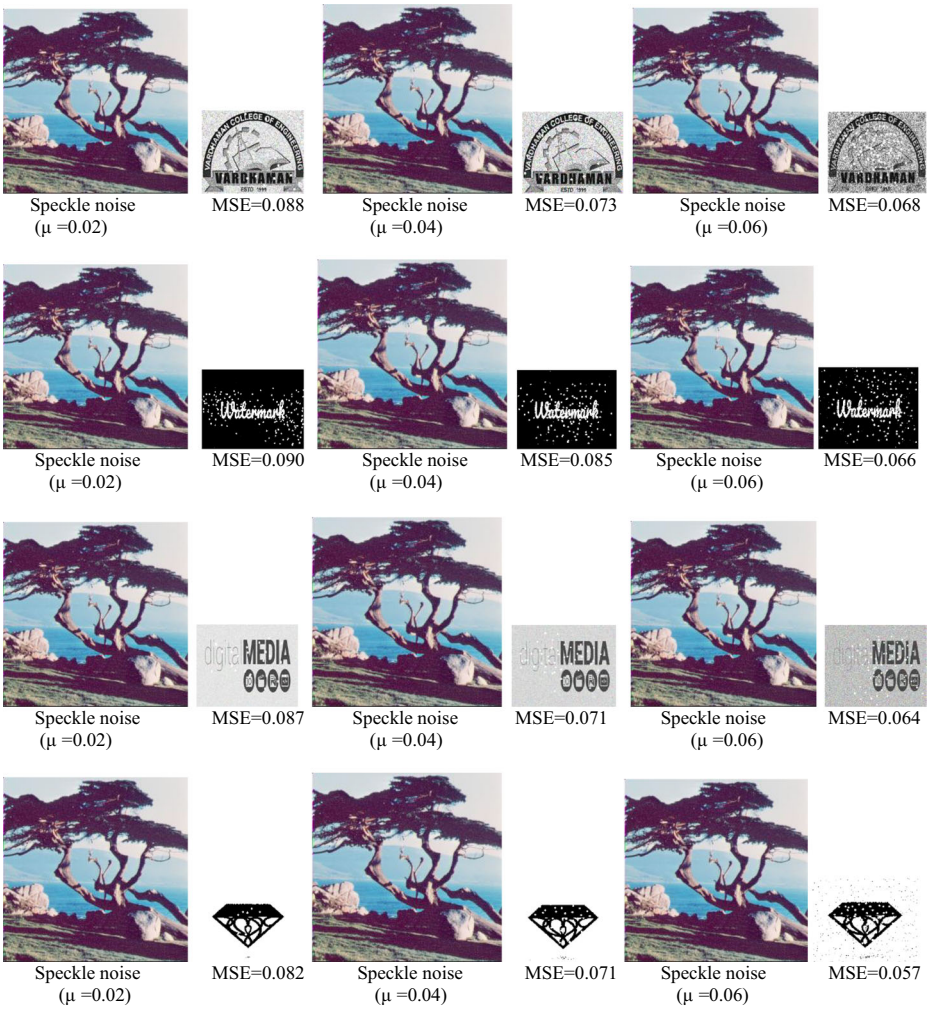


Fig. 14 Extracted watermarks "College logo", "Watermark", "Digital media" and "Diamond" from the attacked "Tree" images against speckle noise

8 Conclusion and future scope

The use of cloud computing environments in multimedia applications has shown a great impact as cutting edge technology to provide unlimited storage for a large amount of multimedia data. The users can access this multimedia content from anywhere, any time as needed and utilize a powerful computing ability and large storage space. Therefore, we have presented a CB-BSWP, which uses a semi-trusted third party for copy deterrence and privacy preservation using cloud computing environments to ensure you can access but cannot leak. In particular, we have used two services of cloud, Infrastructure as a Service (IaaS) to protect the privacy of the participants over the cloud. Watermarking as a service (WaaS) to support the speedy process of watermarking embedding & extracting algorithm and save storage and cost required to store encrypted data. We have used CSP as a "semi-trusted" third party to

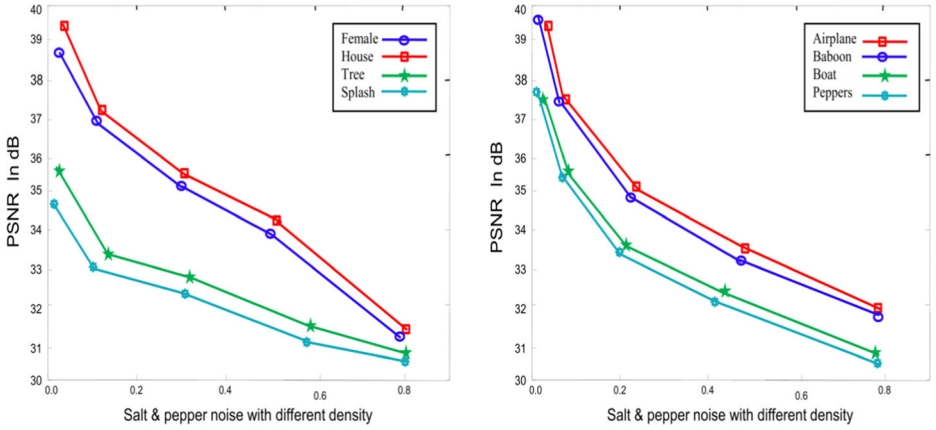


Fig. 15 The PSNR values of watermarked images against salt & pepper noise with different density

strengthen the watermark certificate authority WCA. As, half of the process of watermarking shifted to CSP, resulting in reduced overhead from the WCA and their roles are recognized and valued. The scheme offers a valid solution for the secure distribution of participant's data and preserves their privacy efficiently on the cloud. In our proposed protocol, privacy homomorphism cryptosystem with Diffie-Hellman key exchange is used to create an encrypted domain to ensure the secure exchange of data between buyer and content owner. Our scheme uses robust and fair watermarking to ensure imperceptibility and robustness for the watermarked and watermark images. We have initiated a new scheme for addressing copy deterrence and privacy-preserving problems for a BSWP in cloud computing environment for protecting end-to-end security of digital content over cloud. The key insight of this research work is to strengthen the security of digital content by adopting the privacy homomorphism cryptosystem to squeeze operations for robust and fair watermarking for ensuring high imperceptibility and robustness. We have evaluated the performance of the proposed protocol thoroughly against the requirements and the extracted watermarks were found robust against attacks. In our scheme, the proposed protocol is thoroughly analyzed in section 5 for ensuring security

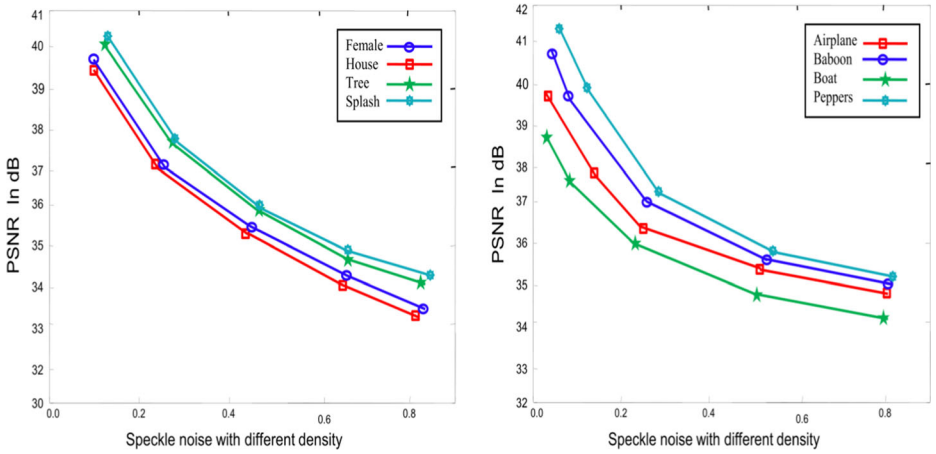


Fig. 16 The PSNR values of watermarked images against speckle noise with different density

strengths of participants, and performance analysis is also provided by comparing the advantages of cloud environment with previously published conventional BSWP protocol which does not use cloud. Extensive experiments have been conducted to evaluate our partially free WCA design, and the results have validated the effectiveness and practicality. Furthermore, the proposed CB-BSWP make a sense theoretically and practically to increase the robustness of the watermark and visual quality of the watermarked images. The result also confirms the novelty of the work to protect digital content security in the field of multimedia applications. In the end some key aspects of the scheme are 1) the proposition of using privacy homomorphism cryptosystem with Diffie-Hellman key exchange algorithm to obtain encrypted domain. 2) CB-BSWP protocol protects end-to-end security of digital content over cloud. 3) SHA-512 algorithm with key size 512-bits to ensure that it doesn't affect computational time. 4) The provision of using fingerprinting based watermarking method to ensure digital rights for the content owner and the customer. 5) Two services of cloud Infrastructure as a service (IaaS) and Watermarking as a service (WaaS) are used. 6) The proposition of using semi-trusted third party for CB-BSWP protocol. The foreseeable future suggests that the online digital content distribution will be more popular and demanded which will definitely need a reliable and dependable copy control mechanism. Anonymity among parties will be a big challenge in the future which requires a robust anonymity control scheme. To generate more robust fingerprints in such a way that it makes it unpractical for an attacker to frame buyer and seller. Computational and communication complexity is still a challenge for the researcher.

Abbreviation *CB-BSWP,* Cloud based buyer seller watermarking protocol; *TTP,* Trusted third party; *IWT,* Integer Wavelet Transform; *ROI,* Regions of Interest; *DRM,* Digital right management; *PKI,* Public key infrastructure; *QoS,* Quality-of-Service; *IaaS,* Infrastructure as a service; *WaaS,* Watermarking as a service; *SHA,* Secure hash algorithm; *WGSP,* Watermark generation and signing phase; *WEVP,* Watermark extraction and verification phase; *PSNR,* Peak signal-to-noise ratio; *MSE,* Mean square error; *dB,* Decibles; $\otimes$, Represent watermarking embedding algorithm

Declarations

Conflict of interest The author declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Mintzer F, Braudaway GW (1999) If one watermark is good, are more better? In: 1999 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings ICASSP99 (Cat. No.99CH36258)
2. Munadi K, Kiya H (2015) A secure online image trading system for untrusted cloud environments. SpringerPlus 4:277
3. Ping Wah W, Memon N (2001) Secret and public key image watermarking schemes for image authentication and ownership verification. IEEE Trans Image Process 10(10):1593–1601
4. Pan W, Coatrieux G (2018) Imperceptible reversible watermarking of radiographic images based on quantum noise masking. Comput Methods Prog Biomed 160:119–128
5. Khan A, Nawaz S (2016) Buyer seller watermarking protocols issues and challenges – a survey. J Netw Comput Appl 75:317–334
6. Naz F, Jeon G (2020) Watermarking as a service (WaaS) with anonymity. Multimed Tools Appl 79(23): 16051–16075
7. Björklund J (2017) A Buyer-seller protocol with watermarking for cloud streaming : towards an ecosystem for media streaming
8. Boneh D et al (2015) Hosting services on an untrusted cloud. Springer, Berlin Heidelberg

9. Liu K, Zhang W, Dong X (2017) A cloud-user protocol based on Ciphertext watermarking technology. Secur Comm Networks 2017:4376282
10. Zhang LY et al (2018) You can access but you cannot leak: defending against illegal content redistribution in encrypted cloud media center. IEEE Trans Dependable Secure Comput:1–1
11. Ren K, Wang C, Wang Q (2012) Security challenges for the public cloud. IEEE Internet Comput 16(1):69–73
12. Shan Z (2018) 51(2) Article p. 31:1–40
13. Zheng Y, Zhou J (2017) Privacy-preserving image Denoising from external cloud databases. IEEE Trans Inform Forensics Secur 12(6):1285–1298
14. World's Biggest Data Breaches & Hacks (2020) Available from: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
15. Armbrust M, Zaharia M (2010) A view of cloud computing. Commun ACM 53(4):50–58
16. Mukwevho MA, Celik T (2018) Toward a smart cloud: a review of fault-tolerance methods in cloud systems. IEEE Trans Serv Comput:1–1
17. Xia Z, Ren K (2016) A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. IEEE Trans Inform Forensics Secur 11(11):2594–2608
18. Zhu J (2010) Cloud Computing Technologies and Applications. In: Furht B, Escalante A (eds) Handbook of Cloud Computing. Springer, Boston, pp 21–45
19. Dong X, Liu K (2018) A cloud-user watermarking protocol protecting the right to be forgotten for the outsourced plain images. Int J Digit Crime For 10(4):118–139
20. Memon N, Ping Wah W (2001) A buyer-seller watermarking protocol. IEEE Trans Image Process 10(4):643–649
21. Peng Y et al (2017) Cloud-based buyer-seller watermarking protocols. In: 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)
22. Qiao L, Nahrstedt K (1998) Watermarking schemes and protocols for protecting rightful ownership and Customer's rights. J Vis Commun Image Represent 9:194–210
23. Zhang X et al (2020) A robust watermarking scheme based on ROI and IWT for remote consultation of COVID-19. Comput Mat Continua 64(3):1435–1452
24. Hsu I-C (2019) XML-Based information fusion architecture based on cloud computing ecosystem. Comput Mat Continua 61(3):929–950
25. Jayashree N, Bhuvaneswaran R-S (2019) a robust image watermarking scheme using Z-transform, discrete wavelet transform and bidiagonal singular value decomposition. Comput, Mater Continua 58(1):263–285
26. Kumar A, Ghrera SP, Tyagi V (2017) An ID-based secure and flexible Buyer-seller watermarking protocol for copyright protection
27. Zeng P, Cao Z, Choo K-KR (2011) An ID-based digital watermarking protocol for copyright protection. Comput Electrical Eng 37(4):526–531
28. Zheng Y, Gui X (2017) Toward encrypted cloud media center with secure deduplication. IEEE Trans Multimedia 19(2):251–265
29. Xiong L, Shim HJ (2019) Secure multimedia distribution in cloud computing using re-encryption and fingerprinting. Multimed Tools Appl 78(21):30297–30313
30. Pass R, Shelat A (2015) Micropayments for Decentralized Currencies, in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. Denver, Colorado, USA, Association for computing machinery, pp 207–218
31. Frattolillo F (2019) A multiparty watermarking protocol for cloud environments. J Inform Securit Appl 47:246–257
32. Leng L et al (2010) Dynamic weighted discrimination power analysis: a novel approach for face and palmprint recognition in DCT domain. Int J Phys Sci 5(17):2543–2554
33. Leng L, Bi X (2017) Dual-source discrimination power analysis for multi-instance contactless palmprint recognition. Multimed Tools Appl 76(1):333–354
34. Chin-Laung L et al (2004) An efficient and anonymous buyer-seller watermarking protocol. IEEE Trans Image Process 13(12):1618–1626
35. Ashwani K (2019) Design of Secure Image Fusion Technique Using Cloud for privacy-preserving and copyright protection. Int J Cloud Appl Comput (IJCAC) 9(3):22–36
36. Chen C-L, Chen PY (2015) A verifiable and secret Buyer–seller watermarking protocol. IETE Tech Rev 32(2):104–113
37. Fontaine C, Galand F (2007) A survey of homomorphic encryption for nonspecialists. EURASIP J Inf Secur 1:013801
38. Rivest RL, Dertouzos ML (1978) On data banks and privacy HOMOMORPHISMS

39. Terelius B (2013) Towards transferable watermarks in buyer-seller watermarking protocols. In: 2013 IEEE International Workshop on Information Forensics and Security (WIFS)
40. Frattolillo F, Buyer-Friendly A (2016) 10(2): p. Article. 9:1–28
41. Leng L, Li M, Teoh ABJ (2013) Conjugate 2DPalmHash code for secure palm-print-vein verification. In: 2013 6th international congress on image and signal processing (CISP). IEEE
42. Leng L, Zhang J (2013) Palmhash code vs. palmphasor code. Neurocomputing 108:1–12
43. Zhang J, Kou W, Fan K (2006) Secure buyer–seller watermarking protocol. IEE Proceedings - Inform Secur 153:15–18
44. Bhattacharya P, Debbabi M, Otrok H (2005) Improving the Diffie-Hellman secure key exchange. In: 2005 International Conference on Wireless Networks, Communications and Mobile Computing
45. Liu KJR et al (2005) Multimedia fingerprinting forensics for traitor tracing
46. Trappe W, Liu KJR (2003) Anti-collusion fingerprinting for multimedia. IEEE Trans Signal Process 51(4): 1069–1087
47. Katzenbeisser S, Veith H (2002) Securing symmetric watermarking schemes against protocol attacks. Electronic. Imaging 4675:SPIE
48. Bianchi T, Piva A (2013) Secure watermarking for multimedia content protection: a review of its benefits and open issues. IEEE Signal Process Mag 30(2):87–96
49. Zhang K, Lu R (2014) Exploiting multimedia services in mobile social networks from security and privacy perspectives. IEEE Commun Mag 52(3):58–65
50. Katzenbeisser S, Maas M (2008) A Buyer–seller watermarking protocol based on secure embedding. IEEE Trans Inform Forensics Secur 3(4):783–786
51. Chang C-C, Tsai H-C, Hsieh Y-P (2010) An efficient and fair buyer–seller fingerprinting scheme for large scale networks. Comput Secur 29(2):269–277
52. Domingo-Ferrer J, Megías D (2013) Distributed multicast of fingerprinted content based on a rational peer-to-peer community. Comput Commun 36(5):542–550
53. Eslami Z, Kazemnasabhaji M, Mirehi N (2014) Proxy signatures and buyer–seller watermarking protocols for the protection of multimedia content. Multimed Tools Appl 72(3):2723–2740
54. Shao M-H (2007) A privacy-preserving buyer-seller watermarking protocol with semi-trust third party, pp 44–53
55. Xie JQ, Xie Q, Tian LJ (2012) A Buyer-seller digital watermarking protocol without third party authorization. Advanc Eng Forum 6-7:452–458
56. Yu Z et al (2012) A novel watermarking method for software protection in the cloud. Software: Pract Exp 42(4):409–430
57. The USC-SIPI Image Database (2020) Available from: http://sipi.usc.edu/database/
58. Cox IJ, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Trans Image Process 6(12):1673–1687

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.