symmetry

MDPI

Article

Vbswp-CeaH: Vigorous Buyer-Seller Watermarking Protocol without Trusted Certificate Authority for Copyright Protection in Cloud Environment through Additive Homomorphism

Ashwani Kumar [1], Mohit Kumar [2], Sahil Verma [3], Kavita [3], N. Z. Jhanjhi [4,*] and Rania M. Ghoniem [5,*]

[1] Department of Computer Science and Engineering, Faculty of Engineering and Technology, SRM Institute of Science and Technology, NCR Campus, Ghaziabad 201204, India
[2] School of Engineering, MIT-ADT University, Pune 412201, India
[3] Faculty of Computer Science and Engineering, SGT University, Gurugram 122505, India
[4] School of Computer Science, SCS, Taylors University, Subang Jaya 47500, Malaysia
[5] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
* Correspondence: noorzaman.jhanjhi@taylors.edu.my (N.Z.J.); rmghoniem@pnu.edu.sa (R.M.G.)

Abstract: Cloud-based storage ensures the secure dissemination of media. Authentication and integrity are important aspects in the distribution of digital media. Encryption-based techniques shelter this media between the communicating parties which are involved in a transaction. The challenge is how to restrict the digital media which is illegally redistributed by the authorized users. However, the digital watermarking technique and encryption-based methods are also not sufficient enough to provide copyright protection. The watermarking protocol is used to provide intellectual property for the customer and the service provider. This research paper provides a vigorous buyer-seller watermarking protocol without trusted certificate authority for copyright protection in the cloud environment. This research work uses the cloud environment which enables the cloud as a service infrastructural provider for storing credentials such as public and private secret keys and the digital certificates of interacting parties. The scheme uses additive homomorphism encryption with an effective key exchange algorithm for exchanging digital media. This proposed approach addresses the problems of anonymity and copy deterrence and protects the digital rights of the buyer and seller; these most up-to-date issues are related to information security. Furthermore, the experiment results conclude that the proposed protocol is flexible and secure even in a non-secure communication channel. We have used performance measures such as PSNR, NCC and cost in time methods for checking the integrity of the proposed protocol. The conducted experiments show a stronger robustness and high imperceptibility for the watermark and watermarked images.

Keywords: cloud environment; privacy-preserving; identity as a service; infrastructure provider

Citation: Kumar, A.; Kumar, M.; Verma, S.; Kavita; Jhanjhi, N.Z.; Ghoniem, R.M. *Vbswp-CeaH:* Vigorous Buyer-Seller Watermarking Protocol without Trusted Certificate Authority for Copyright Protection in Cloud Environment through Additive Homomorphism. *Symmetry* **2022**, *14*, 2441. https://doi.org/10.3390/sym14112441

Academic Editors: Jeng-Shyang Pan and Chin-Ling Chen

Received: 3 October 2022
Accepted: 11 November 2022
Published: 17 November 2022

1. Introduction

Interactive media can be easily stored, distributed and replicated in a digital form, enabling the illegal copying and distribution of digital products [1]. A BSWP integrates watermarking, cryptography and digital signatures to ensure copyright protection [2]. The BSWP basically comes from the field of digital watermarking [3]. Cloud computing is becoming the emerging cutting-edge technology nowadays to provide the secure distribution of data among participants [4]. The issue of customer rights is a problem when duplicate copies of content are found. There have been numerous BSWPs published in the past which use cryptography techniques [5–7]. The previous published BSWP does not use an efficient cloud-based environment for storing the credentials of interacting parties (buyer and seller) or watermarks [8–11]. These existing protocols are not fair for customers and owners. In Salim et al.'s scheme, a visual technique was used to protect the privacy and secrecy of

digital media by identifying and localizing forgeries. They used SIPI datasets for checking the authenticity and performance of the scheme [12]. Pavlović proposed a robust scheme by making use of a jointly trained embedder/detector based on a deep neural network [13]. The embedder is responsible for obtaining imperceptible watermarks, whereas the detector ensures errorless watermark detection. The authors claim that the method achieves high robustness against attacks. Namita et al. proposed a scheme by integrating DCT with a genetic algorithm to achieve highly imperceptible and robust watermarked images [14]. Watermarking methods are used to conceal images and embed this information to the receiver with low distortion. The classification of watermarking, functions, benchmarks and measurements are discussed by Wang and Huang in their research [15,16].

The prime goal of this work is to achieve conceptual modelling for a buyer-seller watermarking protocol. The proposed work is the extension of our previous work [17]. The spatial domain and frequency domain techniques give a better robustness and imperceptibility. Cloud services provide great computation and the secure transmission of digital data. To achieve robustness and fair watermarking, a watermarking system should have requirements such as Kerckhoff's principle, capacity, durability and perceptual quality.

The key goals of our research motivation are given below:

- The protocol is able to address the existing problems associated with the BSWP without making use of a third party; instead, the protocol uses cloud capabilities.
- The proposed protocol shifts all the watermarking process on to the cloud, eliminating the role of a TTP.

This research article is structured as follows. Section 1 represents digital watermarking along with cloud computing technologies. Section 2 reviews the conventional BSWP. In Section 3, the various requirements of the proposed *Vbswp-CeaH* in the cloud environment are shown. Section 4 shows the proposed *Vbswp-CeaH* with a focus on copyright protection in the cloud environment without trusted certificate authority. Section 5 discusses the experimental setup of *Vbswp-CeaH* in the cloud environment, then analyzes the performance of the *Vbswp-CeaH*. Finally, Section 6 concludes the research paper.

2. Reviewing the Conventional BSWP

The process of a BSWP is described as follows. First, the buyer requests a valid watermark from the WCA. Second, the generated watermark for the buyer returns. Third, the buyer sends the purchase order to the seller. Last, the seller delivers the digital content back to the buyer. Zhang et al. proposed a robust deep hiding technique for blind watermarking in 2021. Their approach uses a disentangling forward and backward propagation deep learning approach for an attack simulation layer (ASL) to support data hiding. The authors claim that the proposed approach achieves good performance by adopting a standard ASL inspired by a forward ASL, which is a simple effective method to improve the deep watermarking process [18]. Li et al. proposed that secure watermarking depends on a generative model for concealed attacks. In their approach, the authors use generative networks which consist of an encoder–decoder framework to achieve imperceptibility in the produced digital content. In Pan et al.'s research, a new aggregation function that is named a Network Architecture Probabilistic Aggregation is used to treat the network architectures as graphs [19]. Liu et al. provide a solution against an image encryption which depends on a discrete-time alternating quantum walk (AQW) along with the advanced encryption standard (AES) [20,21].

2.1. Sub-Protocols of Conventional BSWP

A conventional BSWP addresses issues such as copy detection, piracy tracing, man-in-the-middle attacks, customer digital rights and certificate authority issuing [22–26].

2.2. Different Attacks on Security of Conventional BSWP

An attack is any processing that impairs or misleads the watermark detector. Attacks are divided mainly into three parts: attacks on buyer security, attacks on seller security,

and attacks on watermarks. The performance of a watermarking algorithm against these attacks reflects its quality.

2.3. Significance and Motivation

The significance of this research work is to provide a solution without using a trusted third party. The motivation of this research work is to eliminate the role of a trusted third party so that the proposed BSWP with the cloud environment can achieve high flexibility and become light-weighted.

2.4. Security and Usability

To ensure adequate security in a BSWP, the digital media should be encrypted before distribution and uploaded into the cloud in an encrypted manner. The proposed algorithm ensures that only the digital media owner can grant and decrypt the media; no one else can do it. The goal of the proposed algorithm is to prevent the identification of the users without affecting the usability of the compromised digital media.

2.5. Motivation and Contribution

The main contribution of this research work is to provide an effective solution for buyers and sellers to securely exchange digital media without trusted certificate authority in the cloud environment through additive homomorphism. The following are key contributions:

(1) The cloud service provider eliminates the role of trusted certificate authority.
(2) The scheme provides sheltered dealing of digital content over the cloud.
(3) The scheme uses a fingerprinting-based watermarking method to ensure digital rights.
(4) This is a new technique to address the security gaps in the existing watermarking system.

3. Requirements of Proposed *Vbswp-CeaH* in the Cloud Environment

The proposed *Vbswp-CeaH* requires a secure fragile image watermarking scheme, an effective key exchange watermarking scheme and additive homomorphism encryption. This work is the extension of the previous research [17]. The proposed approach uses a fragile watermarking and additive homomorphism encryption-based method to achieve an encrypted domain.

Additive Homomorphism Encryption in the Cloud Environment

There was additive homomorphism encryption in the cloud environment in 1978 [26–28]. Hussain et al. provided a solution for the efficient resource utilization of IoT networks [29,30]. Our scheme adopts additive homomorphism encryption and an efficient key exchange algorithm. The reason to choose additive homomorphic encryption over multiplicative homomorphism encryption is as follows. In the case of multiplicative homomorphism with a small change in plaintext space, it creates a huge difference in ciphertext space. So, to avoid it, we used an addition operation instead of a multiplication operation. The second advantage of an additive homomorphic is that we can store encrypted data in the cloud and perform transforms on it without decrypting it. The following steps are required to achieve secure encryption using additive homomorphism:

Step (1) Select two global public elements $\mathbb{q}$ and α where $\mathbb{q}$ is a prime ($\alpha < \mathbb{q}$) and α is a primitive root of $\mathbb{q}$.
Step (2) Buyer B key generation takes place as follows.

- Select a private key PRk_B where $PRk_B < \mathbb{q}$.
- Calculate the public key PUk_B such that $PUk_B = \alpha^{PRk_B} \bmod \mathbb{q}$

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

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

Step (4) Buyer B calculates the secret key.

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

Step (5) Content owner CO calculates the secret key.

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

Step (6) Feed this secret key K into the additive homomorphism encryption function.

- $D_K(E_K(n) \times (E_K(m)) = n \times m \; OR \; Enc\,(x \otimes y) = Enc(x) \otimes Enc(y)$
- $D_L(E_L(n) \times (E_L(m)) = n + m \; OR \; Enc\,(x \oplus y) = Enc(x) \oplus Enc(y)$

where E_K and D_K are the encryption and decryption algorithm, respectively, with key K.

In this paragraph, the various challenges and design choices for the proposed *Vbswp-CeaH* are given, such as the cloud service provider eliminating the role of the trusted certificate authority. The scheme provides the sheltered dealing of digital content over the cloud. The scheme uses a fingerprinting-based watermarking method which has negotiation mechanisms, and a single watermark insertion is used to ensure digital rights. A new technique to address the security gaps in the existing watermarking system is used. The conventional BSWP addresses issues such as copy detection, piracy tracing, man-in-the-middle attacks, customer digital rights and certificate authority issuing problems without using the cloud environment.

4. Proposed *Vbswp-CeaH* for Copyright Protection

In this section, a BSWP without trusted certificate authority through additive homomorphism is presented. The proposed protocol does not use a trusted third party; instead, it uses the cloud environment for providing secure communication between buyers and sellers, hence ensuring copyright protection. Before outsourcing digital media, it is encrypted using secure additive homomorphism encryption. The protocol uses different services of the cloud environment to eliminate the need for a TTP. The protocol uses Identity as a service (IdaaS) which provides credentials such as public and private secret keys, watermarks and digital certificates. The watermarking embedding process takes place in a secure way because it uses robust watermarking techniques along with PCA, SVD and DWT. The integration of two domains' cloud and image processing enhances the participants' security against various types of attacks which leads to a better performance. The use of the cloud as a repository to store image data allows users to upload images in enormous quantities and of varying sizes. This protocol provides an encrypted domain using the cloud environment without trusted certificate authority for copyright protection. The role of the cloud is vital in our proposed scheme because it reduces communication overheads, saves storage and increases the watermark embedding process i.e., the watermarking bit rate. More specifically, the following research questions are addressed by the protocol. This reported research is an extension of our previous study [17,23,31].

- Why is the Watermark Certificate Authority (WCA) always considered as the TTP?
- Is the protocol still vulnerable to any kind of attack?
- How does replacing the WCA with a content service provider (CSP) make the protocol fast and efficient?

Figure 1 illustrates the framework of the *Vbswp-CeaH*. The authors have used public cloud and cloud instances for carrying out sessions between the buyer and seller. Only watermarked digital content is encrypted on the cloud [32]. We further improved our previous [31] scheme to achieve higher imperceptible images along with Zhang et al. [33].

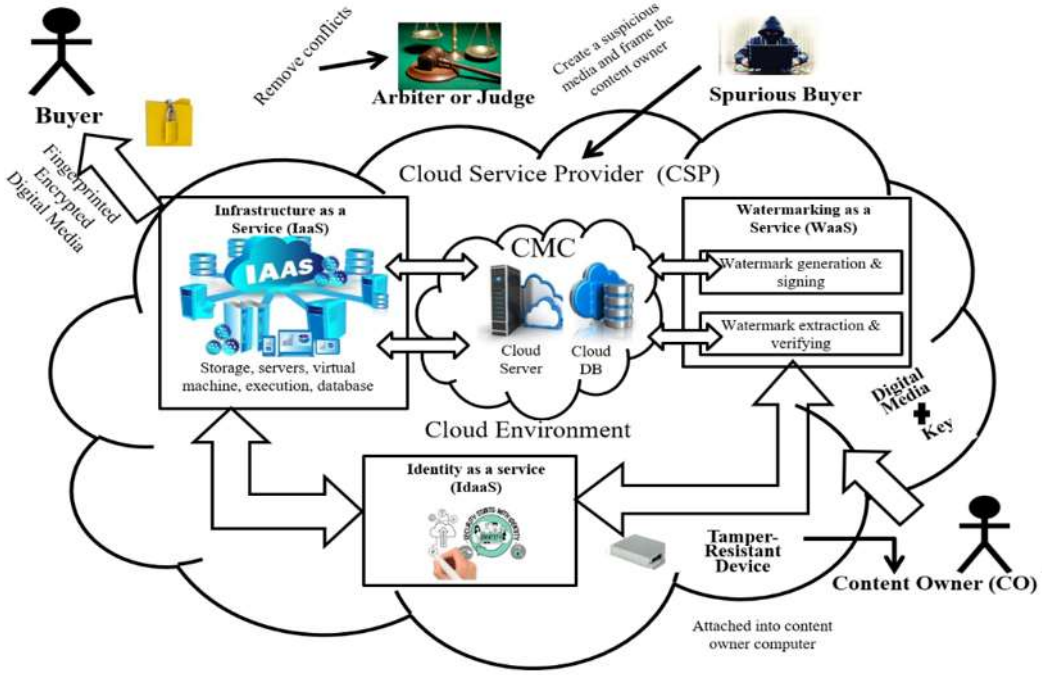

Figure 1. Framework of the *Vbswp-CeaH*.

Figure 2 shows the watermarking scheme applied in the proposed protocol. The watermark can be detected by applying the reverse process of the algorithm. To achieve a fair watermarking scheme, the watermarked bits are embedded using DWT and PCA techniques so that the watermarks can resist against any type of image processing attacks. The cloud computing environment provides a way to restrict the involvement of buyers and sellers to obtain encrypted watermarks. The general process of watermarking is given by [34]. Some previous studies address the problems associated with effective digital watermarking [35–37].

$$DM = \begin{Bmatrix} DM_1 \\ DM_2 \\ DM_3 \\ . \\ . \\ . \\ . \\ DM_n \end{Bmatrix} W = \begin{Bmatrix} W_1 \\ W_2 \\ W_3 \\ . \\ . \\ . \\ . \\ W_n) \end{Bmatrix} \quad (1)$$

$$XDM = \begin{Bmatrix} W_1 \otimes DM_1 \\ W_2 \otimes DM_2 \\ W_3 \otimes DM_3 \\ . \\ . \\ . \\ W_n \otimes DM_n \\ W_{n+1} \otimes DM_{n+1} \end{Bmatrix} \quad (2)$$

where $\otimes$ represents the watermarking embedding function. Equations (2) and (3) show the watermarking system.

$$Enc^N{}_{pk}(XDM) = Enc^N{}_{pk}\begin{Bmatrix} W_1 \otimes DM_1 \\ W_2 \otimes DM_2 \\ W_3 \otimes DM_3 \\ . \\ . \\ . \\ W_n \otimes DM_n \\ W_{n+1} \otimes DM_{n+1} \end{Bmatrix} \quad (3)$$

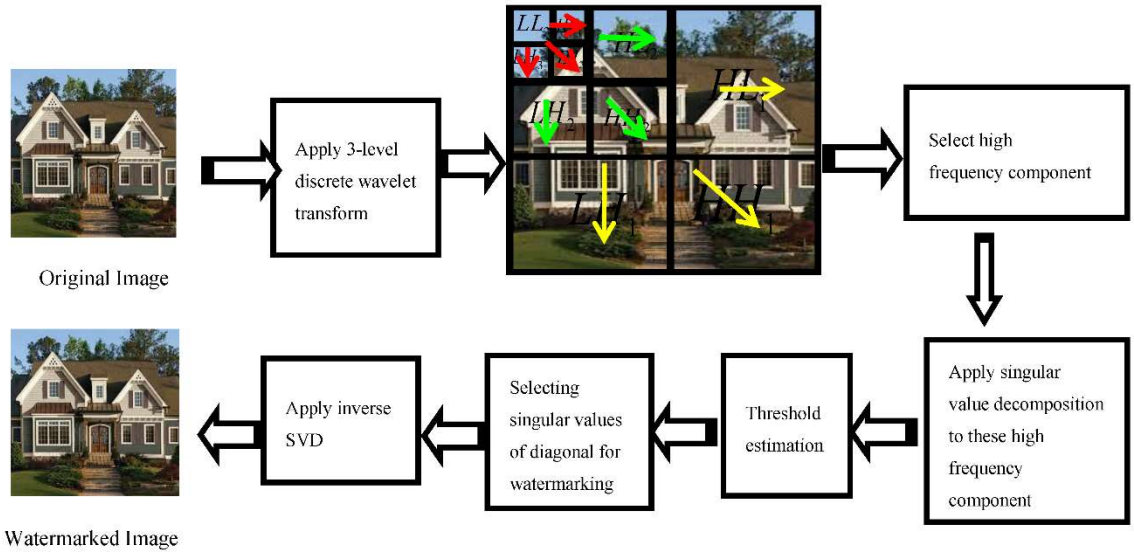

Figure 2. Watermarking scheme applied in proposed protocol.

The encryption system Enc^N is additive homomorphism.

4.1. Registration Process

Before the start of a transaction, each party has to execute the registration process for communication by using a pair of keys $(PRU_B,\ PKR_B)$ and a digital certificate $DS_{UCert_B} = E(PR_{CSP}(ID_{CP}, t, X, W, DM))$. Table 1 shows the complete process of registration.

Table 1. The interaction of buyer and certificate authority.

Buyer B	Certificate Authority CA
B →	: Buyer wants to purchase a digital media.
B→ CA	: M1 = { Request | | IDCO | | CertB}
CA→ B	: $Enc^N\{PR_{CA}(ID_{CO}, t_1, N, W, PU_{B,}Cert_B)\ \}$
B→ CO	: M2 = { N_2 | | IDCO | | CertB}
CO→ B	: $Enc^N[\,PR_{CO}(ID_{CO}, t_2, N, W, PU_{CO,}Cert_{CO})\,]$
B→ CO	: M3 = { Request for Digital Media DM}
CA→	: KeyDH-SHA512(SkCA), $(Rpk_B, Rsk_B)\ N,\ Enc^N{}_{PR_B}(Enc^N{}_{PR_{CA}}(DM))$
CA→ B	: M4 = { $ID_{DM},\ Sk_B$}
CA→ CO	: M5 = { $ID_{DM},\ Pk_B,\ PU_{CO,}\ Sk_{CO},\ E_{PR_{CA}},\ E_{PR_{CA}}(DM)$}
CA→ B	: $DS_{UCert_B} = E(PR_{CA}(ID_{CP}, t, X, W, DM))$

4.2. Algorithm for Secure Watermark Embedding

The Algorithm 1 takes the cover image Cimage and original watermark Woriginal as inputs and performs watermarking embedding for copyright protection. In the below algorithm, the watermarked image C'image is generated by additive homeomorphism encryption $\Phi 2 \leftarrow \Phi 1 \times \Phi 1$ along with the generation of Woriginal by an arbitrary generator which belongs to the $\Phi 1$ group, and the hash function.

Algorithm 1: Algorithm for Secure Watermark Embedding.

Input: C_{image}, $W_{original}$ (cover image, watermark, t, X, DM)
Output: C'_{image}, Pub_{key} (PU_{key})
begin
$C_{image} \rightarrow (W_{original}, \infty, Se_{key}, O_{img})$
$C_{image} \rightarrow (Pub_{key}, \infty)$
$C_{cloud\_env} \rightarrow C'_{image}$, $(Ath_{key})PU_k$
if C'_{image}, = C_{image} + $W_{original} \times PU_{key}$
$\infty \rightarrow$ $Embd_{ing}$ Bits + $W_{original}$
$PR_{CSP} \rightarrow Diff^n(C'_{image} - C_{image})$
$DS \rightarrow E(PR_{CSP}(ID_{CP}, t, X, W, DM))$
PU_{key} (DS)= C'_{image}, Pub_{key}
end If
end

4.3. Algorithm for Watermark Extraction and Authentication

This watermark extraction is used to identify pirated media of the watermarked content. The importance of this Algorithm 2 is to prove the authentication of all users in order to prove copyright protection.

Algorithm 2: Algorithm for Watermark Extraction and Authentication.

Input: C'_{image}, PR_{key} (watermarked image, private key)
Output: C_{image}, W′ (extracted watermark, cover image)
begin
if $(W'_{recovered}) == (W_{original})$
$\infty \rightarrow E(PR_{CSP}(ID_{CP}, t, X, W, DM))$
$DS \rightarrow C'_{image}$, Pub_{key}
if $|C'_{image} - C_{image}|$ <45 db
Resulted watermarked image is considered
if *DS* = Extracted DS
$W'_{original}, \infty, Se_{key}, O_{img} \rightarrow C_{image}$
C'_{image}, $(Ath_{key})PU_k \rightarrow C_{cloud\_env}$
end if
end if
end if
end

The above algorithm is used to identify the illegal distribution of digital media. Whenever there is a need to find out the true owner of the content, this algorithm is executed multiple times for extracting watermarks from the cover images.

5. Results and Discussion Section

5.1. Experimental Setup of Vbswp-CeaH *in the Cloud Environment*

The *Vbswp-CeaH* in the cloud environment was implemented in a MATLAB 2020a environment with a HP LAPTOP 14S-DQ2XXX 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz 2.40 GHz and 8.00 GB RAM. We used a standard dataset available at http://sipi.usc.edu/database (accessed on 17 May 2022). The existing BSWP uses Cox et al.'s [38] method to gain robust watermarking. The efficiency of the protocol was analyzed based on performance measures such as imperceptibility, robustness and cost. For checking the authenticity of the watermarking technique on the suggested protocol, we applied salt and pepper and speckle noise of a variable density to the covered images and watermarked, respectively. Table 2 demonstrate the PSNR values of the obtained results. Figure 3 demonstrate original cover test images of size 512 × 512 used for experiment setup.

Table 2. The PSNR (in dB) values for the proposed *Vbswp-CeaH* protocol.

		Speckle Attack			Salt and Pepper Attack		
Watermarked Images	Original PSNR	0.04	0.06	0.08	0.04	0.06	0.08
"Peppers"	48.06	47.73	46.42	45.23	46.93	44.35	42.66
"House"	47.57	46.67	45.09	44.35	45.81	44.01	43.63
"Boat"	46.65	44.12	43.43	41.87	45.04	44.86	43.89
"Fishing Boat"	49.97	48.96	47.91	46.23	49.23	48.46	47.23

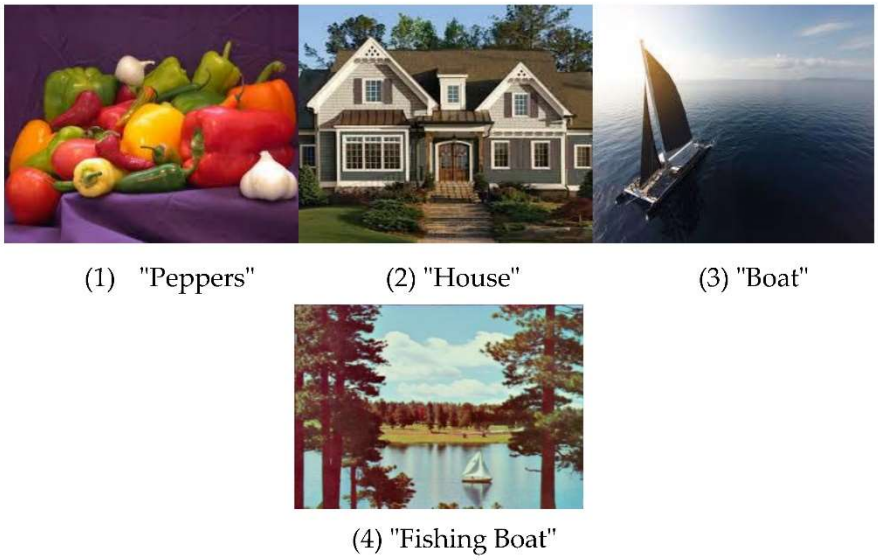

Figure 3. Cover test images, size 512 × 512.

Figure 4a–c are the test watermark images used conducting the experiments of proposed vigorous buyer-seller watermarking protocol without trusted certificate authority for copyright protection in cloud environment through additive homomorphism. Figure 5 shows the various recovered watermarked images from the attacked images.

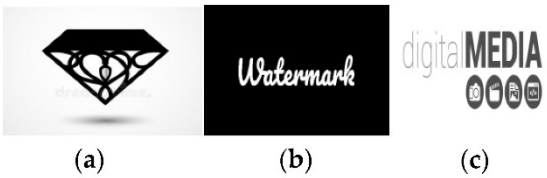

Figure 4. Figure (**a**–**c**) are the test watermark images used for simulation.

Figure 6 shows the various recovered watermarked images from the attacked images of Salt & pepper noise. In Figure 7, we show the PSNR values obtained from the simulation of the effective watermarking scheme in the cloud environment. We used geometric attacks on the covered and watermarked images with different density. The proposed scheme does not report any perceptual degradation on the watermarked images; the watermark is also still recoverable with good NCC values.

5.2. Performance Analysis of Vbswp-CeaH *in the Cloud Environment*

In this section, the simulation result of the *Vbswp-CeaH* is shown. The efficiency of the protocol was analyzed using performance measures such as the No. of watermarked images embedded into the digital media and the time taken for embedding and extraction. The instances of cloud were used for carrying out sessions between buyers and sellers. These performance metrics affect the cost and bandwidth for every digital media content retrieved from the cloud in an encrypted domain [39].

Figure 8 represents the watermarked images in different environments such as cloud environment, client-side local computer and in hybrid cloud. We compared our proposed

protocol with the traditional protocol, as depicted in Table 3 which shows a detailed comparison of *Vbswp-CeaH* in the cloud environment with conventional BSWP solutions. We tested performance against problems involving anonymity (AP), tamper detection (TD), non-framing (NFP), non-repudiation (NRP), customer rights (CRP), traceability (TP) and unbinding (UP).

Figure 5. Recovered watermarks from the attacked "Peppers" and "Home" images.

Figure 6. Recovered watermarks from the attacked "Boat" and "Fishing Boat" images.

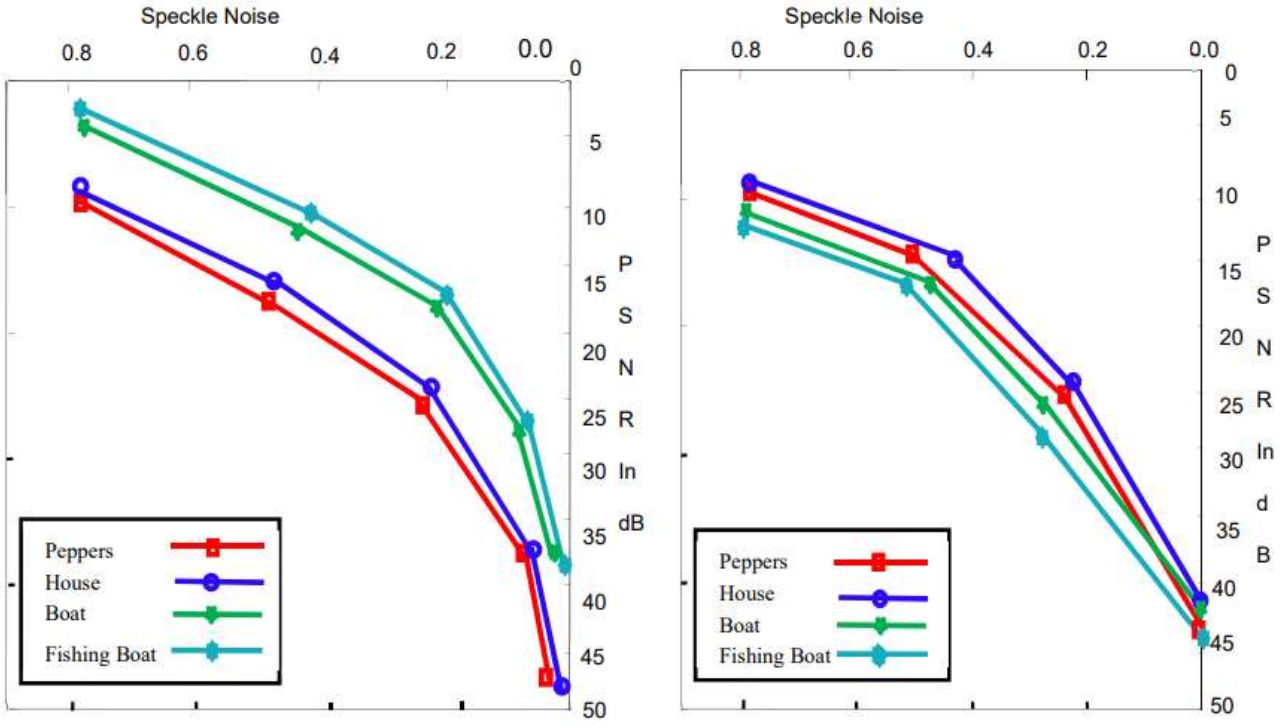

Figure 7. The PSNR values of the cover objects against salt and pepper noise.

Figure 7 represent the PSNR values of the cover object against speckle noise with different noise density. These images show the relationship between the cover object and the noise.

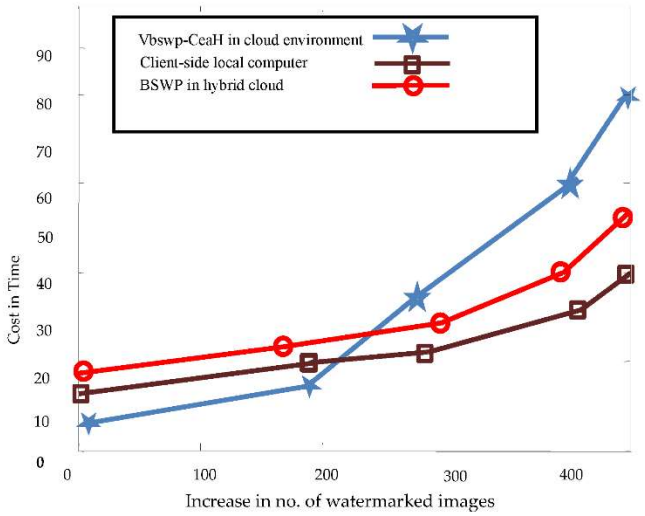

Figure 8. The watermarked images in different environments.

6. Conclusions

In this paper, a cloud computing environment was used for the processing of watermarked images, storing them in an encrypted domain and preventing unauthorized access. This paper shows a new technique to address the security gaps in the existing watermarking system. The main contribution of this article is to ensure the safe transmission of data in the cloud environment, filter out fraudulent users and provide copyright protection for all parties involved in the transaction. The proposed protocol uses the cloud environment which enables a cloud-based watermarking scheme for ensuring robustness, imperceptibility and cost effective. By using the advantages of cloud computing such as the cloud as a service infrastructural provider for storing the credentials of buyers and sellers

and the processing of the watermark generation and extraction and other services required for the interaction of buyers and sellers which makes the protocol efficient and secure. The enforcement of the protocol was evaluated, and extracted watermarks stand robustly against the attacks. The result show that the protocol achieves great computation power and secures storage in the cloud. In addition, researchers should focus on developing advanced methods such as IoT and blockchain-based authentication.

Table 3. Comparison of *Vbswp-CeaH* in cloud environment with previously published BSWPs [23,31,33,40–46].

S.N.	Conventional BSWP	Security Problems Solved by *Vbswp-CeaH* in Cloud Environment					
		AP	**NFP**	**NRP**	**CRP**	**TP**	**UP**
1	Yu et al. (2012)	✗	✓	✓	✓	✓	✗
2	Shao (2007)	✓	✓	✓	✗	✗	Not Reported
3	Xie et al. (2012)	✗	✓	✓	✓	✓	✗
4	Kumar et al. (2017)	✗	Not Reported	✓	✗	✓	✓
5	Chang et al. (2010)	✓	✓	Not Reported	✓	✓	✗
6	Kumar (2019)	✗	✓	✓	✗	Not Reported	Not Reported
7	Domingo-Ferrer and Megías (2013)	✓	✓	✓	Not Reported	✗	Not Reported
8	Zhang et al. (2006)	Not Reported	✓	✓	✗	✓	Not Reported
9	Frattolillo et al. (2016)	✓	✓	✓	✗	✓	✓
10	Eslami et al. (2014)	✓	Not Reported	✓	✗	✓	✓
11	**Proposed *Vbswp-CeaH* in Cloud Environment**	✓	✓	✓	✓	✓	✓

Author Contributions: Conceptualization, A.K.; methodology, M.K.; formal analysis, S.V.; investigation K.; resources, N.Z.J.; data curation, R.M.G.; writing—original draft, A.K.; writing—review and editing, M.K.; visualization, S.V.; supervision, K.; funding acquisition, N.Z.J.; and R.M.G. All authors have read and agreed to the published version of the manuscript.

Funding: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R138), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data will be provided upon request.

Acknowledgments: We sincerely acknowledge the support from Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R138), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflict of interest.

Abbreviations

Vbswp-CeaH	Vigorous buyer-seller watermarking protocol without trusted certificate authority for copyright protection in cloud environment through additive homomorphism
BSWP	Buyer-seller watermarking protocol
PSNR	Peak signal-to-noise ratio
NCC	Normalized cross-correlation
CSP	Content service provider
WCA	Watermark certificate authority
DCT	Discrete cosine transform
TTP	Trusted third party
PCA	Principal component analysis
DWT	Discrete wavelet transform
SVD	Singular value decomposition
dB	Decibels

References

1. Goi, B.-M.; Phan, R.C.-W.; Yang, Y.; Bao, F.; Deng, R.H.; Siddiqi, M. Cryptanalysis of two anonymous buyer-seller watermarking protocols and an improvement for true anonymity. In *International Conference on Applied Cryptography and Network Security*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3089.
2. Memon, N.; Ping Wah, W. A buyer-seller watermarking protocol. *IEEE Trans. Image Process.* **2001**, *10*, 643–649. [CrossRef] [PubMed]
3. Chin-Laung, L.; Pei-Ling, Y.; Pan-Lung, T.; Ming-Hwa, C. An efficient and anonymous buyer-seller watermarking protocol. *IEEE Trans. Image Process.* **2004**, *13*, 1618–1626.
4. Zhu, J. Cloud Computing Technologies and Applications. In *Handbook of Cloud Computing*; Furht, B., Escalante, A., Eds.; Springer: Boston, MA, USA, 2010; pp. 21–45.
5. Mukwevho, M.A.; Celik, T. Toward a Smart Cloud: A Review of Fault-tolerance Methods in Cloud Systems. *IEEE Trans. Serv. Comput.* **2018**, *14*, 589–605. [CrossRef]
6. Lv, Z.; Qiao, L.; Verma, S.; Kavita. AI-enabled IoT-Edge Data Analytics for Connected Living. *ACM Trans. Internet Technol.* **2021**, *21*, 1–20. [CrossRef]
7. Kumar, M.; Raju, K.S.; Kumar, D.; Goyal, N.; Verma, S.; Singh, A. An efficient framework using visual recognition for IoT based smart city surveillance. *Multimed. Tools Appl.* **2021**, *80*, 31277–31295. [CrossRef] [PubMed]
8. Kumar, S.; Shanker, R.; Verma, S. Context Aware Dynamic Permission Model: A Retrospect of Privacy and Security in Android System. In Proceedings of the 2018 International Conference on Intelligent Circuits and Systems (ICICS), Phagwara, India, 19–20 April 2018; pp. 324–329. [CrossRef]
9. Terelius, B. Towards transferable watermarks in buyer-seller watermarking protocols. In Proceedings of the 2013 IEEE International Workshop on Information Forensics and Security (WIFS), Guangzhou, China, 18–21 November 2013.
10. Peng, Y.; Hsieh, Y.; Hsueh, C.; Wu, J. Cloud-based buyer-seller watermarking protocols. In Proceedings of the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, San Francisco, CA, USA, 4–8 August 2017.
11. Dash, S.; Verma, S.; Kavita; Bevinakoppa, S.; Wozniak, M.; Shafi, J.; Ijaz, M.F. Guidance Image-Based Enhanced Matched Filter with Modified Thresholding for Blood Vessel Extraction. *Symmetry* **2022**, *14*, 194. [CrossRef]
12. Salim, M.Z.; Abboud, A.J.; Yildirim, R. A Visual Cryptography-Based Watermarking Approach for the Detection and Localization of Image Forgery. *Electronics* **2022**, *11*, 136. [CrossRef]
13. Pavlović, K.; Kovačević, S.; Djurović, I.; Wojciechowski, A. Robust Speech Watermarking by a Jointly Trained Embedder and Detector Using a DNN. *Digit. Signal Process.* **2022**, *122*, 103381. [CrossRef]
14. Agarwal, N.; Singh, P.K. Discrete cosine transforms and genetic algorithm based watermarking method for robustness and imperceptibility of color images for intelligent multimedia applications. *Multimed. Tools Appl.* **2022**, *81*, 19751–19777. [CrossRef]
15. Wang, F.H.; Pan, J.S.; Jain, L.C. Digital Watermarking Techniques. In *Innovations in Digital Watermarking Techniques. Studies in Computational Intelligence*; Springer: Berlin/Heidelberg, Germany, 2009; Volume 232. [CrossRef]
16. Pan, J.-S.; Huang, H.-C.; Jain, L.C. *Intelligent Watermarking Techniques*; World Scientific Pub Co Inc.: River Edge, NJ, USA, 2004.
17. Kumar, A. A cloud-based buyer-seller watermarking protocol (CB-BSWP) using semi-trusted third party for copy deterrence and privacy preserving. *Multimed. Tools Appl.* **2022**, *81*, 21417–21448. [CrossRef]
18. Zhang, C.; Karjauv, A.; Benz, P.; Kweon, I.S. Towards Robust Deep Hiding Under Non-Differentiable Distortions for Practical Blind Watermarking. In Proceedings of the 29th ACM International Conference on Multimedia Association for Computing Machinery, Virtual, China, 20–24 October 2021; pp. 5158–5166.
19. Pan, Z.; Hu, L.; Tang, W.; Li, J.; He, Y.; Liu, Z. Privacy-Preserving Multi-Granular Federated Neural Architecture Search A General Framework. *IEEE Trans. Knowl. Data Eng.* **2021**, 1. [CrossRef]
20. Liu, G.; Li, W.; Fan, X.; Li, Z.; Wang, Y.; Ma, H. An Image Encryption Algorithm Based on Discrete-Time Alternating Quantum Walk and Advanced Encryption Standard. *Entropy* **2022**, *24*, 608. [CrossRef] [PubMed]
21. Zhu, D.; Zheng, J.; Zhou, H.; Wu, J.; Li, N.; Song, L. A Hybrid Encryption Scheme for Quantum Secure Video Conferencing Combined with Blockchain. *Mathematics* **2022**, *10*, 3037. [CrossRef]
22. Kumar, A. *A Review on Implementation of Digital Image Watermarking Techniques Using LSB and DWT Information and Communication Technology for Sustainable Development*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 595–602.
23. Kumar, A. Design of Secure Image Fusion Technique Using Cloud for Privacy-Preserving and Copyright Protection. *Int. J. Cloud Appl. Comput.* **2019**, *9*, 22–36. [CrossRef]
24. Kumar, A.; Srivastava, S. Object Detection System Based on Convolution Neural Networks Using Single Shot Multi-Box Detector. *Procedia Comput. Sci.* **2020**, *171*, 2610–2617. [CrossRef]
25. Kumar, A.; Reddy, S.S.S.S.; Kulkarni, V. An Object Detection Technique For Blind People in Real-Time Using Deep Neural Network. In Proceedings of the 2019 Fifth International Conference on Image Information Processing (ICIIP), Shimla, India, 15–17 November 2019; pp. 292–297. [CrossRef]
26. Ghosh, G.; Sood, M.; Verma, S. Internet of things based video surveillance systems for security applications. *J. Comput. Theor. Nanosci.* **2020**, *17*, 2582–2588. [CrossRef]
27. Tian, X.; Huang, Y.; Verma, S.; Jin, M.; Ghosh, U.; Rabie, K.M.; ThuanDo, D. Power allocation scheme for maximizing spectral efficiency and energy efficiency tradeoff for uplink NOMA systems in B5G/6G. *Phys. Commun.* **2020**, *43*, 101227. [CrossRef]

28. Dash, S.; Verma, S.; Kavita; Khan, M.S.; Wozniak, M.; Shafi, J.; Ijaz, M.F. A Hybrid Method to Enhance Thick and Thin Vessels for Blood Vessel Segmentation. *Diagnostics* **2021**, *11*, 2017. [CrossRef]
29. Hussain, A.; Nazir, S.; Khan, F.; Nkenyereye, L.; Ullah, A.; Khan, S.; Verma, S. A resource efficient hybrid proxy mobile IPv6 extension for next generation IoT networks. *IEEE Internet Things J.* **2021**. [CrossRef]
30. Pass, R.; Shelat, A. Micropayments for Decentralized Currencies. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015. [CrossRef]
31. Kumar, A.; Ghrera, S.P.; Tyagi, V. An ID-based Secure and Flexible Buyer-seller Watermarking Protocol for Copyright Protection. *Pertanika J. Sci. Technol.* **2017**, *25*, 57–76.
32. Liu, Y.; Tang, S.; Liu, R.; Zhang, L.; Ma, Z. Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Syst. Appl.* **2018**, *97*, 95–105. [CrossRef]
33. Zhang, J.; Kou, W.; Fan, K. Secure buyer–seller watermarking protocol. *IEEE Proc.-Inf. Secur.* **2006**, *153*, 15–18. [CrossRef]
34. Liu, K.; Zhang, W.; Dong, X. A Cloud-User Protocol Based on Ciphertext Watermarking Technology. *Secur. Commun. Netw.* **2017**, *2017*, 4376282. [CrossRef]
35. Zhang, L.Y.; Zheng, Y.; Weng, J.; Wang, C.; Shan, Z.; Ren, K. You Can Access But You Cannot Leak: Defending against Illegal Content Redistribution in Encrypted Cloud Media Center. *IEEE Trans. Dependable Secur. Comput.* **2018**, *17*, 1218–1231. [CrossRef]
36. Wang, J.; Wan, W.B.; Li, X.X.; De Sun, J.; Zhang, H.X. Color image watermarking based on orientation diversity and color complexity. *Expert Syst. Appl.* **2020**, *140*, 112868. [CrossRef]
37. Wang, S.-S.; Yan, K.-Q.; Wang, S.-C. Achieving efficient agreement within a dual-failure cloud-computing environment. *Expert Syst. Appl.* **2011**, *38*, 906–915. [CrossRef]
38. Cox, I.J.; Kilian, J.; Leighton, F.T.; Shamoon, T. Secure spread spectrum watermarking for multimedia. *IEEE Trans. Image Process.* **1997**, *6*, 1673–1687. [CrossRef]
39. Katzenbeisser, S.; Lemma, A.; Celik, M.U.; van der Veen, M.; Maas, M.A. Buyer–Seller Watermarking Protocol Based on Secure Embedding. *IEEE Trans. Inf. Forensics Secur.* **2008**, *3*, 783–786. [CrossRef]
40. Chang, C.-C.; Tsai, H.-C.; Hsieh, Y.-P. An efficient and fair buyer–seller fingerprinting scheme for large scale networks. *Comput. Secur.* **2010**, *29*, 269–277. [CrossRef]
41. Domingo-Ferrer, J.; Megías, D. Distributed multicast of fingerprinted content based on a rational peer-to-peer community. *Comput. Commun.* **2013**, *36*, 542–550. [CrossRef]
42. Eslami, Z.; Kazemnasabhaji, M.; Mirehi, N. Proxy signatures and buyer–seller watermarking protocols for the protection of multimedia content. *Multimed. Tools Appl.* **2014**, *72*, 2723–2740. [CrossRef]
43. Frattolillo, F. A Buyer-Friendly and Mediated Watermarking Protocol for Web Context. *ACM Trans. Web* **2016**, *10*, 1–28. [CrossRef]
44. Shao, M.-H. A Privacy-Preserving Buyer-Seller Watermarking Protocol with Semi-trust Third Party. In *International Conference on Trust, Privacy and Security in Digital Business*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 44–53.
45. Xie, J.Q.; Xie, Q.; Tian, L.J. A Buyer-Seller Digital Watermarking Protocol without Third Party Authorization. *Adv. Eng. Forum* **2012**, *6–7*, 452–458. [CrossRef]
46. Yu, Z.; Thomborson, C.; Wang, C.; Wang, J.; Li, R. A cloud-based watermarking method for health data security. In Proceedings of the 2012 International Conference on High Performance Computing & Simulation (HPCS), Madrid, Spain, 2–6 July 2012.