A blockchain based buyer-seller watermark protocol with trustless third party

Chunlin Song[1,2], Hong Wang[2], Wei Zhang[2], Sud Sudirman[3], Haogang Zhu[1*]
[1] State Key Laboratory of Software Development Environment, Beihang University, Beijing, China
[2] BOE Technology Group Co.Ltd, Beijing, China
[3] Department of Computer Science, Liverpool John Moores University, Liverpool, UK
Chunlin.song@hotmail.com, wanghong@boe.com.cn, drzhangwei@boe.com.cn, s.sudirman@ljmu.ac.uk, haogangzhu@buaa.edu.cn

Abstract
With the development and innovation of digital information technologies and new-generation Internet information platforms, new types of information exchange methods have been spawned. It has broken the restriction of the traditional internet boundary, and integrated all round connections between people and objects. Based on the above progresses, digital multimedia contents distributed or published much more convenient on the internet than before and most of them without any copyright protection. The dishonest owner can easily copy and distribute the digital multimedia content without reducing any perceptual quality. According to the relative concerns, watermark protocol networks play a very important role on usage tracking and copyrights infringement authentication etc. However, most of the watermark protocols always require a “fully trusted third party”, which has a potential risk to suffer conspiracy attack. Therefore, in this paper, we focus on designing a watermark protocol with trustless third party via blockchain for protecting copyrights of owners that they want to publish or distribute on the internet. The proposed watermark protocol includes three sub-protocols which covers the negotiation process, transaction process and identification processes. In addition, this paper also provides a fully detail analysis that describes the benefits and weaknesses of current solution.

Keywords:
Watermark protocol, copyright protection, blockchain, multiparty, trustless third party

1. Introduction
With the rapid development of intelligence, network and communication technology, the relative digital multimedia products are infiltrated into all aspects of social life. In the other words, the development of new technologies has brought new development opportunities to the digital publishing and digital copyright industries, and the proportion of digital publishing in the entire publishing industry has also grown rapidly. The new form of digital publishing has brought tremendous pressure and challenges to digital copyright protection.

Digital Rights Management (DRM) is the main method for copyright protection of digital works transmitted on the network. It is defined by the American Publishers Association: "Technologies, tools and processes for protecting intellectual property rights in the process of digital content transactions." Watermark protocols as one of the DRM techniques which designed as a system solution by applying information security technology to ensure the legitimate and authorized users use digital multimedia contents (such as digital images, audio, video, etc.) normally. The watermark protocol protects the entire circulation process of digital content from production to distribution, sales to use. Specifically, it keeps eyes on the various processes of describing, identifying, trading, protecting, monitoring, and tracking the various forms of use of digital assets.

The traditional centralized DRM system might apply a central data server as a data repository to store and manage digital content. In the classic “buyer-seller” two-party watermark protocol, the fully trust-third party or semi-trust-third party as a favorite architecture has attracted by different researchers [1-8]. The third parties involved in the protocols in the real world have to be concerned as “untrusted” since they could collude with the other parties, thus impairing security [9].

In order to design a watermark protocol with trustless third party, we introduce blockchain network as one of the core techniques in the proposed watermark protocol. The blockchain is a distributed databased that contains an ordered list of records linked together through chains, on blocks. It maintains a continuous growing list of records which are immutable. Due to this reason, the proposed watermark protocol builds on the blockchain technology achieve secured distribution of assets among untrusted parties [11].

This paper is organized as follows. Section 2 describes main problems and existing solution. Section 3 describes the preliminaries of blockchain. Section 4 discusses the proposed watermark protocol in detail. Section 5 designs the experiments and then, section 6 analyses the benefits and weakness of the proposed watermark protocol. Finally, final remarks are described in section 6.

2. Main Problems and Existing Solution

During the transaction process of different digital product, the trust problem as the most important complications has been concerned, which can be divided into the following categories: customer's rights problem, unbinding and anonymous problem, conspiracy problem.

2.1.The first trust problem -- customer's rights problem

Identification of unauthorized copy as the primary mean to resolve copyright protection problems of traditional watermark protocol. In these solutions, the content owner inserts the watermark signals into the digital multimedia content to detect the dishonest customer during the process of transaction. In these schemes, the seller is assumed as the only trustworthy party which is responsible for inserting and extracting the fingerprint signal. However, in real world, the above assumptions are not fully guaranteed. The seller attempts to frame consumer maliciously by inserting a specific watermark signal and spreading the digital contaminated multimedia content as an unapproved copy. From another point of view, a buyer whose watermark has been located in an unauthorized copy could declare that the seller created the unauthorized copy in order to frame the buyer. In the absence of sufficient safeguards to avoid such issues and legally sound procedures to confirm or deny that such infringements have taken place. This problem is popularly known as the Customer's Rights problem.

To best of our knowledge, all of the existed well-known watermark protocol systems are attempted to solve the customer's rights problem. Qiao and Nahrstedt propose the first watermark protocol in 1998 [12]. In this protocol, an encrypted watermark signal is provided for embedding into digital content as the first step. After that, the watermarked content is sent to the consumer. And then, the consumer request to a trusted third party to provide the authorization by decrypting the watermarked content and extracting the unique message. This protocol provides one of a kind of solutions for resolving the Customer's Rights problem, however, it does not protect the customers fully from subsequent potential problems that may arise from unauthorized use of the digital watermarked contents.

2.2 The second trust problem -- anonymous and unbinding problem

The watermark protocol mechanism is failed due to the unique watermark signal could not bind to a specific copy of the digital content in whole transaction process, this situation is referred as unbinding problem. This problem could lead to where a watermark is transplanted from a copy of low-priced digital content to another copy of higher-priced digital content to fabricate piracy from the side of dishonest seller. The buyer's identity is failed to be protected in the transaction process of watermark protocol unless any guilt can be proven. This concerns is signified as anonymous problem. The possible solution shows that the buyer's identity is bind with a unique certificate from the trusted third party or certification agency.

The first solution of anonymous and unbinding problem is addressed by C.Lei et. al [1]. It contains three subprotocol which includes registration subprotocol, watermarking subprotocol and arbitration subprotocol. In the first sub-protocol, the customer applies for an anonymous certificate in the certification center with encryption system. Then, an anonymous certificate is generated from certification center with public key and sent it to the customer. After that, two different watermark signals are inserted into digital content through six different steps. Finally, the arbitration sub-protocol is executed whenever a suspected pirated copy of the product is found.

2.3 The third trust problem -- conspiracy problem

Conspiracy problem is defined as two or more untrusted parties are colluded to fabricate piracy. In fact, multiple conspirators could combine their watermark signals for removing the original watermark signals or generating a new version of digital watermarked content, which detectors unable to trace any of the real colluders involved.

J. Choi first proposes a two-party of buyer-seller watermark protocol in 2003 to avoid conspiracy problem [14]. In this protocol, the mechanism only involves two parties, buyer and seller. In order to take care of the other problems, the system applies secure commutative cryptosystems to watermark protocol. The similar solution also presents by Zhang et al in 2006 [15]. However, the trusted third part are still considered in plenty of the other researches' work because of there are two reasons need to be considered [10]:

- At least one trusted third party is involved to validate specific data;
- The buyer performs complex security actions if the trusted third party is limited or tag as untrusted

To sum up, the trust problem has always been an important fact affecting human development, customer's rights problem, anonymous and unbinding problem, conspiracy problem as the main issues for affecting the copyright. The trust system is still dominated by transaction process, lack of trust is due to privacy issues, IT security and performance risks. Blockchain technology refers as the technical solution of collectively maintaining a reliable database through decentralization and de-trusting. The characteristics of blockchain are unforgeable, traceable, transparent which act as one of the most important factors to resolve the trust problem and it could be applied into watermark protocols.

3. Preliminaries

3.1 Basic Concept

A blockchain can be recognized as a decentralized shared ledger which combines different data blocks to become a specific data structure through chains. All the related information is safety collected, stored in a certain sequence, and transferred transparently which can be verified in the system. In another words, blockchain technology is a new type of decentralized infrastructure and distributed computing structure which using encrypted chain block structure to verify and store data, using consensus algorithms in different distributed node to generate and update data and using smart contracts to program and implement [16].

In a blockchain, each new transaction is announced to a distributed network of nodes; the transaction is added to a block if all nodes are approved. A timestamp, the hash of the previous block and the transaction data as the main elements in every block, and different blocks linked together to create an immutable, append-only chain. Copies of the entire blockchain are maintained by each participating node. The characteristics is described as follows and the details of blockchain could be found [17]:

- Decentralization: Blockchain is a distributed database without central node that contains an ordered list of records linked together through chains, on blocks. Blocks can be defined as individual components that contain same information relating to a particular transaction. A blockchain network maintains a continuous growing list of different records.
- Immutable: In each blockchain, a transaction information has a corresponding hash value. The hash value

combines each record to compose a sub-node and to generate a binary Merkle tree. In addition, the root node of Merkle tree, timestamp and the identifier are stored in the block header to form chain structure. Therefore, if the records in one block are attempted to be modified by dishonest parties or conspirators, the rest of blocks in the entire chain are required to be modified. In general, if there are more than six blocks are generated in the entire chain, it can be considered as tamper-resistant.

- Unforgeable: The digital signatures of different parties during transaction process with cryptographic system are also stored in the blockchain for making sure the entire architecture unforgeable.
- Traceable: The behaviors of all involved parties are traceable, and these behaviors are permanently saved in the blockchain, therefore, it is impossible to withdraw the related information once the behavior is completely.

Blockchain technology is intended to decentralize transaction processing between different centers. For achieving this target and applied to different fields, the smart contract is required to apply.

3.2 Smart Contract

The concept of smart contract is first proposed by American scientist Nick Szabo in 1994 which is defined as "a computerized transaction protocol that enforces contracts term" [18]. In other words, any contracts/transaction process have been pre-programmed with a set of definitive rules and regulations in order to reduce the demand in the execution of ordinary contracts. However, due to the social environment at that time, the smart contract is not widely applied until the blockchain technology is exposed. Fig.1 illustrated the work mechanism of smart contract

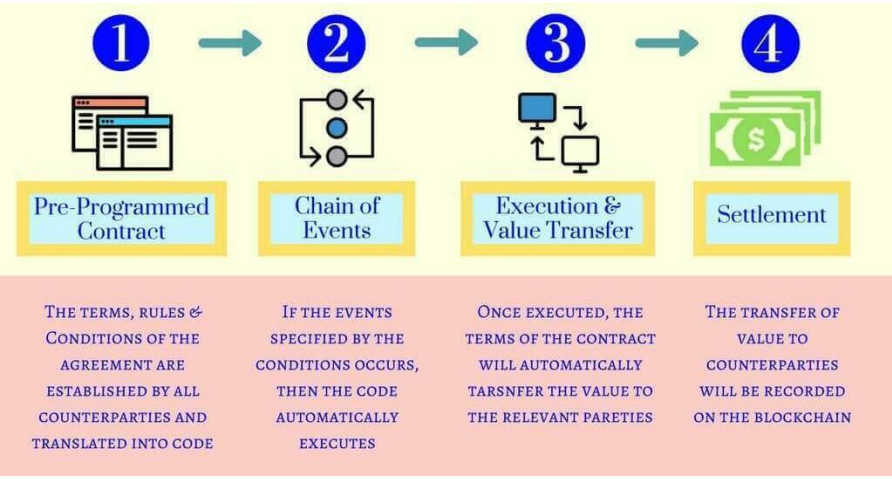

Figure 1. The work mechanism of smart contract [20]

4. Watermark Protocol

4.1 Main Goal

As we discussed in the above section, in this paper, we present a new watermarking protocol based digital right management by using blockchain technology, smart contract technology and watermark protocol technology. A decentralized watermark protocol is established by applying blockchain technology in a peer-to-peer network that does not require a trust third-party organization. The digital content is stored in the IPFS to solve the data security problem. The use of the smart contract enables the watermark protocol to perform transaction process in real time, efficiently and automatically. The proposed watermarking protocol is based on our previous work [27] and also draws on the experience of Frrattoillo's work [21] which aims:

1. To fulfil the buyer-seller requirement with trustless third party
2. To introduce blockchain technology to solve a series of trust problem

3. To guarantee only one watermark signal insertion in the business transaction

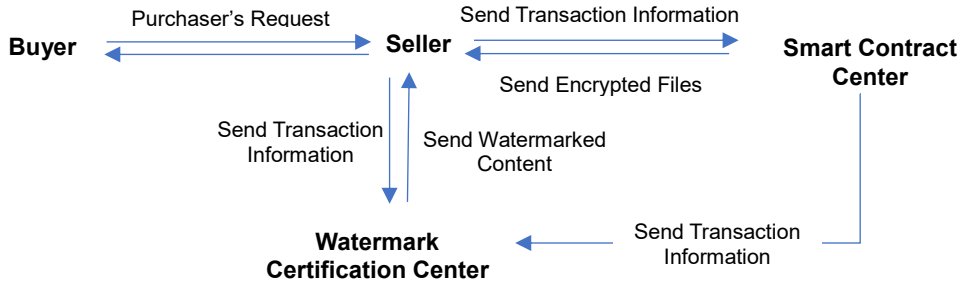

Figure 2. The structure of proposed watermark protocol

In this section, a buyer-seller watermark protocol is proposed. It consists of three sub-protocols: 1). negotiation subprotocol; 2) watermark subprotocol and 3) identification and arbitration subprotocol, the structure of proposed scheme is shown in Fig.2. In addition, there are 4 different parties are involved which is introduced in Table I and the denotations of different symbols are demonstrated in Table II.

Table I. The notations of different parties in this protocol

Notations	Description
B	The buyer who wants to purchase the digital contents
S	The seller who wants to sell the digital contents.
SCC	Smart contract center integrates reliable and secure transactions with web application, it will also perform the smart contract.
WCC	The watermark certification center is responsible for generating watermark signal, it is assumed to supply specialized watermarking and security service.

Table II. Notations used in the watermark protocol description

Symbol	Meaning
X	Digital contents
B_{id}	Buyer's identify
S_{id}	Seller's identify
X_B	brief description of digital product X
$\bar{X}$	Watermarked X
id_{SCC}	Identify of smart contract center
$E_{Key}(\ldots)$	Encrypted by using the key and a public crypto-system
$(pk_N^X,\ sk_N^X)$	A public-private key pair belonging to entity N.

4.2 Watermark Protocol

4.2.1 Negotiation Subprotocol

1. The subprotocol starts with the buyer B who visits the sell's S website or the third-party platform and chooses a digital product X, then B delivers the request message m_1 to S and to send buyer identify B_{id} with its digital signature and timestamp to smart contract center SCC;

2. After receiving the purchase request, S bind the product identifier X_B and its identify S_{id}, then, S signs X_B digitally with its secret key sk_s, and sent it with digital product X and timestamp as message m_2 to SCC.
3. SCC receives the messages B_{id} and m_2, verifies the identify of B and S, if the data is incorrect or the buyer/seller is recorded in the blacklist, the transaction is disclosed. Otherwise, SCC generates two pairs of public and private key, (pk_B^X, sk_B^X) and (pk_S^X, sk_S^X) which have to be used to identify X_B in the current transaction.
4. SCC encrypts B_{id}, S_{id}, pk_B^X, sk_B^X, pk_S^X, sk_S^X, X_B, id_{SCC}, with its public key pk_{SCC} to generate E_{SCC}. After that, SCC sends message m_3 to buyer, m_4 to seller and m_5 to WCC with digital signature and timestamp. The first message m_3 includes X_B and sk_B^X, m_4 includes pk_B^X, pk_S^X, sk_S^X, X_B, id_{SCC} and E_{SCC}, the latter message m_5 includes B_{id}, pk_B^X, pk_S^X to WCC.
5. Call the smart contract center to write data to blockchain and the negotiation protocol is completed

4.2.2 Watermark Subprotocol

1. The seller receives the message m_4 and verify the signature id_{SCC}, the transaction is aborted if the information incorrect. Afterward, it encrypts the digital content X with seller's public key pk_S^X to create $E_{pk_S^X}(X)$ and sends it to WCC with identify S_{id} and digital content description X_B.
2. WCC generate a watermark signal which depend on the two particular functions m and n, it produces two different binary string, x and y, respectively. The first labels the buyer on the basis of B_{id} and S_{id}, whereas the latter is depended on X_B and T_{WCC}. Hence, x =m(B_{id} + S_{id}) and y = n(X_B + T_{WCC}). Whereas f is a unique m-bit random value. Therefore, the unique watermark is represented as $W = \mu + \sigma + f$.
3. Then, pk_B^X, pk_S^X and privacy homomorphic cryptosystem are applied to achieve a double encryption of W and X, the $E_{pk_B^X}(E_{pk_S^X}(W))$ and $E_{pk_B^X}(E_{pk_S^X}(X))$ are created.
4. The encrypted watermark signal is directly inserted into encrypted digital content by exploiting the homomorphism of the encryption scheme. Finally, the encrypted digital watermarked content is illustrated as below:

$$E_{pk_B^X}(E_{pk_S^X}(\bar{X})) = E_{pk_B^X}(E_{pk_S^X}(X \oplus W))$$

5. Once the encrypted digital watermarked content is produced, WCC sends it to S with its digital signature and timestamp. In addition, WCC stores X_B, pk_S^X, pk_B^X, and $E_{pk_B^X}(E_{pk_S^X}(\bar{X}))$ in a new entry of TableX and broadcasted to all distributed network
6. S receives the encrypted content of digital watermarked content, then $E_{pk_B^X}(E_{pk_S^X}(\bar{X}))$ is decrypted by using private key sk_S^X and commutative cryptosystem to get $E_{pk_S^X}(\bar{X})$ and send to B.
7. B accepts $E_{pk_S^X}(\bar{X})$ and use its private key sk_B^X to decrypt it to obtain the digital content $\bar{X}$, which is the final and protected version of X.
8. The payment is followed the previous step between buyer and seller.
9. Call the smart contract center to write data to blockchain and the watermark protocol is completed

4.2.3 Identification and arbitration Subprotocol

Whenever a pirated copy of a protected content X' is found in the market. Identity the responsible distributor is the major job in this period. Therefore, WCC could start to implement this protocol immediately by verify the digital content X'.

1. At the first step, the seller S sends X' to WCC.
2. The extraction algorithm is executed for extracting the watermark W' at WCC.
3. WCC retrieves its database and uses W' to search them as a match. If the related information is found, WCC retrieves the related evidence X_B, pk_S^X, pk_B^X, $E_{pk_B^X}(E_{pk_S^X}(\bar{X}))$ and sends them to SCC as message m_1 with the description of content X', denoted as $descr_{X'}$
4. SCC received m1 and verify whether all information is corrected, then it decrypts and extracts B_{id}, S_{id}, pk_B^X,

sk_B^X, pk_S^X, sk_S^X, X_B, and compare the related information. Then SCC will decide whose the guilty party is. Otherwise, the protocol ends without exposing and identify.

5. Experiments

This section is the experiment part which aims to verify the blockchain based watermarking protocol. There are two experiments contained in this section. The first experiment runs the watermarking algorithm and illustrated the watermarked digital product. The second experiment focus on the prototype of whole system.

5.1 Watermark Experiment

The result of the watermarking experiment as the first part of experiment is presented. Any robust watermarking algorithms are would like to apply to any kind of digital product such as digital videos and audios, digital images or digital games etc. For demonstrating the results of the proposed watermarking protocol, in this part, we applied a robust DWT-SVD watermarking technique described in [28] into the proposed models, the image 'lena' as the host image and digital product is shown in Fig.3a, Fig.3b is the watermark image which embeds into digital product in WCC, Fig.3c shows the final watermarked product after insertion.

(a) (b). (c)

Figure 3 (a) The host image (b) The watermark image (c)The watermarked content after insertion

As a quantitative measure of the degradation effect caused by the attacks we use Peak-Signal-to-Noise Ratio (PSNR). The PSNR compares the original watermarked signal and the modified watermarked signals. High PSNR values indicate lower degradation. In our experiment, the PSNR value achieves 37.8.

5.2 Prototype

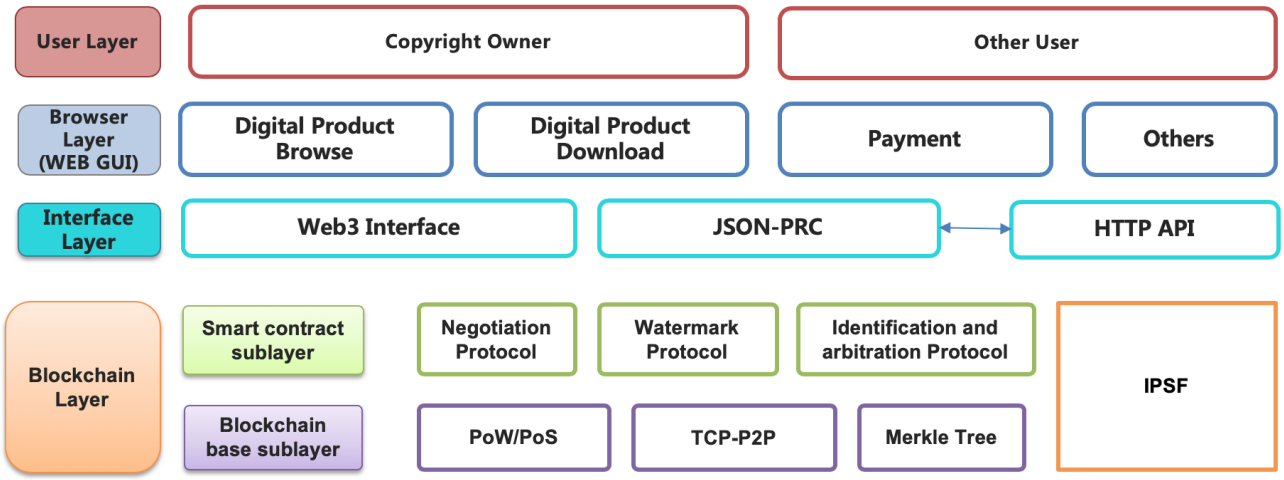

Figure 4 Architecture of the platform implementing the proposed watermark protocol

In the foundation of the whole process, the cloud computing platform is supposed to be apply to support the "Infrastructure as a Service" service. It executes a variety of processes with OpenStack API to our watermarking

protocol.

The architecture of the platform includes blockchain layer, interface layer, browser layer and user layer which is shown in Fig.4. In blockchain layer, there are two different sub-layers are consisted that is blockchain based sublayer and smart contract sublayer. In the blockchain sublayer, the Ethereum technology as the basis of the whole architecture is supposed to apply, the transaction data is supposed to be written into the underlying blockchain, except the digital product itself. Smart contract sublayer will automatic execute the steps of watermark protocol that include negotiation subprotocol, watermark subprotocol and identification & arbitration subprotocol. The smart contract layer interacts with browser layer through the interface layer. The browser layer provides different graphic functions as interface to different graphical user. The user layer is divided into two classier: copyright owner and other user, it refers to the various users using the system. They are communicated with the other middle layer through wired or wireless network for complete the whole transaction process.

6. Security Analysis and Discussion

6.1 Objectives Review

The proposed watermark protocol has been designed with trustless third party, it applies blockchain technology for achieving all goals:

(1) To design the buyer-seller watermark protocol with trustless third party
(2) The trust problem is solved which is introduced in section 2
(3) Only one watermark signal insertion in the business transaction

For achieving the above targets, there are 4 main reasons which are described below: first of all, the decentralized distributed ledger is applied. In our proposed scheme, there are various parties are joined the transaction, each party could be recognized as a node, and each node keeps a complete and same account. The novel and decentralized bookkeeping scheme is differed from the traditional way, it indicates that all nodes record the same accounts, and therefore, it avoids to audit false accounting from any single node. On the other hands, the security of the account data is guaranteed due to enough accounting nodes.

Secondly, forge a non-existent record is almost impossible except more than 51% of the accounting nodes are controlled. When there are enough nodes are joined into the blockchain network, the system eliminates the possibility of counterfeiting. The modification of the database on a single node is invalid, so the data stability and reliability of the watermark protocol is extremely high.

Thirdly, the transaction information stored on the watermark protocol and blockchain system is open and public, therefore, any party could query the related data, the information in the entire system is highly transparent. At the same time, the identity is highly encrypted and could only be accessed with the authorization of the owner, thereby, the data is security and personal privacy.

Finally, the blockchain uses consensus-based algorithm to allow all nodes in the entire system to interchange securely in a trustless environment. In addition, the protocol imposes an explicit requirement that messages are always exchanged over secure and anonymous communication channels between different parties through an SSL connection, which are generally provided by web browsers and guarantee a high security level. Furthermore, digital signatures and timestamps are used in the protocol to control the ongoing transactions.

In order to improve the efficient of whole watermark protocol. There is one watermark signal commissioned to instead of more than two watermark signals at traditional architecture [25, 26]. On the premise of solving the unbinding attack, one watermark insertion could improve the hidden capacity and avoids ambiguity attack.

6.2 Comparison with other protocols

Lei et al. first applies homomorphic cryptosystem in his buyer-seller watermark protocol [1]. In this protocol, the trusted third party -- WCC inserts watermark signals and to guarantee a correct copyright process. In fact, the protocol implements the correct authentication of buyers without exposing their identities during the transaction process. Thus, the protection of the buyers' privacy is guaranteed, and the sellers could not gather privacy data during the transaction.

The unbinding problem has been concerned and a number of subsequent watermark protocols work on it which includes [5, 7]. But, these protocols are affected by the double watermark insertion problem [3]. Double watermark insertion as an accepted and suitable solution for solving the unbinding problem. However, a limited capacity including hiding information of digital content needs to be considered. On the other hand, a single watermark insertion not only provide a robust and secure outcome, but also allow to insert long bit string codes that is particularly helpful to reach anti-collusion target [3, 6, 9]

Table III. The summary of watermark protocols

Requirements fulfilled	[1]	[5]	[7]	[3]	Proposed Protocol
Unbinding	√	√	√	√	√
No Repudiation	√	√	√	√	√
Collusion Tolerance	√	√	√	√	√
No framing	√	√	√	√	√
Anonymity	√	√	√	√	√
Traceability	√	√	√	√	√
One Watermark Insertion	×	×	×	√	√
Trustless Third Party	×	×	×	×	√

Compared with the above solutions, this paper also avoids conspiracy attack and protects different entities copyright by applying different encrypt algorithms. Furthermore, there are two specific functions are used to generate two binary codes which are then combined to produce a single watermark. The summary of prominent watermark protocols and their fulfillment of the buyer's and seller's requirement is given in Table III.

In the future, the second-hand market even or the third-hand market business transaction should be concerned. The dishonest owner could distribute the copy of digital content freely without reduce any quality. Currently, there is only one watermark protocol research paper introduce the experience for the second-hand and third-hand market [27]. Further standardized and develop the second-hand market would make a contribute to protect the rights and interests of different parties.

7. Conclusion

Currently, the world is moving into the digital decade, and in new age, digital multimedia contents distributed or published are much more convenient on the internet than before and most of them without any copyright protection. Therefore, in this paper, we proposed a buyer-seller watermark protocol via blockchain for protecting copyrights of owners that they want to publish or distribute on the internet. The proposed watermark protocol consists of three sub-protocols that covers the registration process, transaction process and identification processes. In addition, the trustless third party as the brightest spot is considered which avoid conspiracy attack successfully. Besides that, the rest of the problems such as copyright's protection, unbinding problem and cost-effective are also contemplated.

Reference

[1]. C. L. Lei et al., “An efficient and anonymous buyer-seller watermark protocol,” IEEE Transaction on Image Process,13(12),1618–1626, 2004.

[2]. F. Frattolillo. "Watermark protocol for web context". IEEE Transaction on Information Forensics and Security, 2(3), 350-363, 2007.

[3]. D. Hu, Q. Li. "A secure and practical buyer-seller watermark protocol". International Conference on Multimedia Information Networking and Security, 105-108, November, 2009.

[4]. A. Rial, M. Deng, T. Bianchi, A. Piva and B.Preneel. "A provably secure anonymous buyer-seller watermark protocol", IEEE Transaction on Information Forensics and Security, 5(4), 920-931, 2010.

[4]. A. Rial, J. Balasch, B. Preneel. "A privacy-preserving buyer-seller watermark protocol based on priced oblivious transfer", IEEE Transaction on Information Forensics and Security, 6(1), 202-212. 2011.

[5]. Y. Peng, C. Wang, Y. Fang and W. Li. "Anonymous watermark protocol for vector spatial data", International Conference on Computer Science & Service System, 2095-2098, Nanjing, 2012.

[6]. F. Frattolillo. "Watermark protocol: problems, challenges and a possible solution". The Computer Journal, 58(4), 944-960, 2014.

[7]. C. Chen, C. Chen, D. Li and P. Chen. "A verifiable and secret buyer-seller watermark protocol". IETE Technical Review, 32(2), 104-113, 2015.

[8]. J. Huang, F.Jeng, T.Chen. "A new buyer-seller watermark protocol without multiple watermarks insertion". Multimedia Tools and Applications, 1-13, 2016.

[9]. F. Frattolillo. "A buyer-friendly and mediated watermark protocol for web context". ACM Transactions on the Web, 10(2), Article 9, 2016.

[10]. A. Rial, M. Deng, T. Bianchi, A. Piva, and B. Preneel. A provably secure anonymous buyer-seller watermark protocol. IEEE Transactions on Information Forensics and Security 5(4), 920–931, 2010.

[11]. Q. Xia, E. Sifah, K. Asamoah, J.Gao, X. Du, M. Guizani. MeDShare: Trustless medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757-14767.

[12]. L. Qiao, K. Nahrstedt, Watermarking schemes and protocols for protecting rightful ownership and customer's rights. Journal of Visual Communication and Image Representation, 9(3), 194-210, 1998.

[13]. N. Memon and P. W. Wong, “A buyer-seller watermark protocol”, IEEE Transaction on Image Process, 10(4), 643–649, 2001.

[14]. J. Chio, K. Sakurai, J. Park. Does it need trusted third party? Design of buyer-seller watermark protocol without trusted third party. International Conference on Applied Cryptography and Network Security, 265-279, 2003.

[15]. J. Zhang, W. Kou, K. Fan. Secure buyer-seller watermark protocol. IEEE Proceedings on Information Security, 153(1), 15-18.

[16]. R. Beck, J. Czepluch, N. Lollike, S.Malone. Blockchain—the gateway to trust-free cryptographic transactions. Proceedings of the 24th European Conference on Information Systems, 1-14, 2016

[17]. M. Pilkington. Blockchain technology: principles and applications. Research Handbook on Digital Transformations, Technique Report, 2015.

[18]. Smart Contracts. Available online: https://web.archive.org/web/20011102030833/http://szabo.best.vwh.net:80/smart.contracts.html (accessed on 13 January 2020).

[19]. Factom whitepaper. Business processes secured by immutable audit trails on the blockchain. https://github.com/FactomProject/FactomDocs/blob/master/Factom_Whitepaper_v1.2.pdf.

[20]. What is A Smart Contract? https://www.jianshu.com/p/d776f37acd1f.

[21]. F. Frattolillo. A multiparty watermarking protocol for cloud environments. Journal of Information Security and Applications, 47, 246-257, 2019.

[22]. P. Lee, M. Awad, E. Leiss. A practical, almost zero-knowledge watermark verification algorithm. International Journal of Engineering and Technology, 8(1), 9-16, 2016.

[23]. M. Ghadi, L. Laouamer, L. Nana, A novel zero-watermarking approach of medical images based on

Jacobian matrix model: a novel zero-watermarking approach of medical images, Security and Communication Networks, 9(18), 5203-5218, 2016.
[24]. X. Kang, G. Lin, Y. Chen, F. Zhao, E. Zhang, C. Jing. Robust and secure zero-watermarking algorithm for color images based on majority voting pattern and hyper-chaotic encryption. Multimedia Tools and Applications, 2019.
[25]. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren. A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing, IEEE Transactions on Information Forensics and Security, 2016.
[26]. Z. Zhou, Y. Wang, J. Wu, C. Yang, X. Sun, Effective and efficient global context verification for image copy detection, IEEE Transactions on Information Forensics and Security, 2016.
[27]. C. Song, J. Sang and S. Sudirman. A buyer-seller watermarking protocol for digital secondary market, Multimedia Tools and Application, 77(2), 225-249, 2018
[28]. C. Song, S. Sudirman and M.Merabti. A robust-adaptive dual image watermarking technique, Journal of visual communication and image representation, 23, 549-568, 2012.