applied sciences

MDPI

Article

A Novel and Robust Hybrid Blockchain and Steganography Scheme

Mustafa Takaoğlu [1,*], Adem Özyavaş [2], Naim Ajlouni [2], Ali Alshahrani [3] and Basil Alkasasbeh [3]

[1] Department of Computer Engineering, Istanbul Aydın University, 34295 Istanbul, Turkey
[2] Department of Software Engineering, Istanbul Atlas University, 34413 Istanbul, Turkey; adem.ozyavas@atlas.edu.tr (A.Ö.); naim.ajlouni@atlas.edu.tr (N.A.)
[3] Department of Computer Engineering, Arab Open University, Riyadh 11681, Saudi Arabia; a.shahrani@arabou.edu.sa (A.A.); bkasasbah@arabou.edu.sa (B.A.)
* Correspondence: mustafatakaoglu@aydin.edu.tr; Tel.: +90-4441-428-684-05

Abstract: Data security and data hiding have been studied throughout history. Studies show that steganography and encryption methods are used together to hide data and avoid detection. Large amounts of data hidden in the cover multimedia distort the image, which can be detected in visual and histogram analysis. The proposed method will solve two major drawbacks of the current methods: the limitation imposed on the size of the data to be hidden in the cover multimedia and low resistance to steganalysis after stego-operation. In the proposed method, plaintext data are divided into fixed-sized bits whose corresponding matching bits' indices in the cover multimedia are accumulated. Thus, the hidden data are composed of the indices in the cover multimedia, causing no change in it, thus enabling considerable amounts of plaintext to be hidden. The proposed method also has high resistance to known steganalysis methods because it does not cause any distortion to the cover multimedia. The test results show that the performance of the proposed method outperforms similar conventional stenographic techniques. The proposed Ozyavas–Takaoglu–Ajlouni (OTA) method relieves the limitation on the size of the hidden data, and hidden data is undetectable by steganalysis because it is no longer embedded in the cover multimedia.

Keywords: steganography; blockchain; OTA data hiding algorithm; blockchain steganography; proof of work

Citation: Takaoğlu, M.; Özyavaş, A.; Ajlouni, N.; Alshahrani, A.; Alkasasbeh, B. A Novel and Robust Hybrid Blockchain and Steganography Scheme. *Appl. Sci.* **2021**, *11*, 10698. https://doi.org/10.3390/app112210698

Academic Editor: Paula Fraga-Lamas

Received: 19 October 2021
Accepted: 9 November 2021
Published: 12 November 2021

1. Introduction

Steganography [1] is a working principle that emerges from the moment it is realized that information is valuable and needs to be hidden. At its core lies the concealment of information inconspicuously [2]. There are known examples of steganography that have been carried out by many methods throughout history [3]. For example, steganography methods have been known, such as tattooing the information to be hidden onto a slave's scalp after their hair has been cut, sending the message to the person to whom the message will be delivered after the slave's hair grows back, or transmitting the information using wax tablets [4].

With the advancement of technology and the emergence of new opportunities, steganography studies are also developing in this direction [5]. Likewise, with a better understanding of the possibilities of using blockchain technology, it is seen that steganography can be used together with blockchain [6–8]. Blockchain technology has emerged as a suitable subject for steganography studies with its distributed architecture, anonymity, and data security [9,10].

Blockchain technology is a joint study of computer science and cryptology [11]. Blockchain systems have a decentralized structure [12,13]. Each of the nodes that make up the system has an up-to-date version of the blockchain data. For this reason, data are distributed systemically to resist attacks [14]. Hash functions link the blocks that make

up the blockchain system [15,16]. Because these functions work unilaterally and give different values in case of any tampering, they keep the system security at the highest level [17]. Since the introduction of Bitcoin in 2009 by Satoshi Nakamoto, the importance of blockchain technology has been better appreciated, and studies have been carried out on its application areas. Blockchain technology can be added to existing systems as a layer, or it is possible to find examples developed using only blockchain. Blockchain systems can be developed using Bitcoin, Ethereum, and Hyperledger, and many similar platforms [18]. In addition, without using these platforms, blockchain systems can be developed using programming languages such as JavaScript, Solidity, and Java [19]. Under special circumstances, systems are designed where it is possible to add your own desired features. Due to such possibilities, blockchain technology is a study subject used in many areas, such as finance, transportation, public services, identification, and authentication.

In the literature review of this study, it can be seen that traditional methods of digital steganography are utilized to achieve similar results obtained in the blockchain technology. Considering the profound effect of Bitcoin crypto money on the financial sector, blockchain technology should introduce new methods into steganography. For this reason, it is necessary to fully understand the capabilities of blockchain technology and to identify innovative methods to meet steganographic needs.

Various methods are used to measure the success of steganography methods and to detect stego-data as it is not realistic for humans to detect and analyze the steganography methods used today. For this reason, many computerized steganalysis methods are used to detect steganography-applied multimedia stego-data [20].

The essence of steganography is the concealment of information, and it is not necessary to do this hiding process with conventional methods [21]. Hence, this study proposes the Ozyavas–Takaoglu–Ajlouni, OTA blockchain steganography algorithm. The proposed method uses hybrid steganography with blockchain technology. With the OTA algorithm, all steganalysis methods used today will be invalidated. The OTA algorithm does not cause any distortion to the cover image, and it performs the information hiding process with an algorithm developed iteratively. This study has a literature review, materials and methodology, analysis, results, and discussions sections.

2. Literature Review

The Stego-chain method, proposed by Sarkar et al. [22], was presented with Robert's edge detection method. This study aims to increase the embedding payload by expanding the edge areas in the image. The stego-image obtained after the steganography process was encrypted with the Advanced Encryption Standard (AES). Later, this file was divided into small frames and sent to the receiver over the blockchain. After obtaining the stego-image from the frames, the receiver uses the key to follow the reverse steps and retract the information. Adequate technical information has not been shared regarding the process of confirming and recording the transactions by other nodes on the blockchain and the award and the reliability logic they recommend. The tables and images shared regarding the blockchain in the study are not satisfactory. In this study, the steganography part is much stronger and is of great importance as it is one of the few indexed studies published in blockchain steganography.

Mohsin et al. [23] proposed minor changes to the Particle Swarm Optimization (PSO) algorithm to protect and transmit COVID19 data through blockchain technology securely. The algorithm used more than one cover -image. In this algorithm, the optimal data storage locations were detected and used for each image. Hash values are added to stego-images to maintain integrity. In a blockchain system, tamper-proofing stego-images with added hash values will do the same job with increased complexity. A well-known feature is that a transaction approved by blockchain nodes is removed from the system in case of changes or tampering. In addition, the first and second pieces of information shared in the Claims and Limitations sections of the article are shared information that cannot be counted as being correct.

Basuki and Rosiyadi [24] successfully developed a secure data transmission system with a transaction steganography and image steganography method. Traditional image steganography is carried out with encrypted confidential information using the Ethereum system in which information such as partition number, image URL, and access time is created. With transaction steganography, they used three stages: transaction field selection, the embedding method, and the parsing method. They carried out unique work that can be exemplified as blockchain steganography. The authors examined steganography and blockchain systems very accurately in their studies and successfully used them in the proposed system.

Partala [25] proposed a powerful system using blockchain and Least Significant Bit (LSB) in his cover communication study. This system realizes the result of the sender transmitting the information to the other party as a result of a series of transactions by hiding 1 bit of data in each transaction. The blockchain system was designed correctly, and the steganography was accomplished. The only thing that can be seen as a weakness in this study is time, as it takes more than one hour of data time to send approximately 1 byte of data. Making one transaction for each bit can also cause very high transaction numbers in large data. The proposed method outperforms all the other methods it has been compared with in the literature.

Horng et al. [26] encoded the cover images they determined with the RDHEI method they proposed using block permutation. They also concealed the encrypted patient data in the cover image, which they encrypted using the histogram shifting method. This method is carried out in the blockchain system; secure data transmission is ensured, and the embedding rate is provided at a level of 0.8 bits per pixel (bpp). In an environment with a large amount of patient data, such as a hospital, the resolution of the hidden images is high. In other words, in a data set where the size of the secret data is large, the operating time of the blockchain system, encryption processes, and steganography steps in the proposed system will take a very long time.

Xu et al. [27] proposed a steganography study with a method they developed over public blockchain transactions. It creates a new block by performing a series of operations on selected transactions and recording this steganographic information in the new block. The applicability of this study raises some questions because, today, in many systems with a public blockchain, it is not possible for miners to create blocks if they do not have a very strong processing power. Most importantly, they are unlikely to create a block in the way they proposed and save it as the new block in a public blockchain because new transaction information is created and recorded in line with the features introduced in the genesis block of each blockchain. Mazdutt et al. [28] revealed that 1600 transaction records were made in the Bitcoin Blockchain that did not resemble the data produced by the system. These data entries can be easily detected, and studies are underway to prevent such data records. Xu et al. did not state how to save the stego-data they created in the block structure of a public blockchain without being noticed.

Giron et al. [29] proposed a steganalysis method. Their study is used to determine steganography methods using steganalysis techniques on the blockchain system. However, despite their extensive research and examination, they could not find any evidence of steganography on public blockchain systems. However, some observations were made on the misuse of steganography in the blockchain steganography studies suggested in the literature. They tried the steganalysis methods, which they call Sequential analysis and Clustering analysis, on 625,941 Bitcoin and 6 million Ethereum blocks and 98 million bitcoin clusters. The study revealed that more work is needed in this area.

When the blockchain steganography was examined in the literature, the pros and cons of the proposed methods were considered, but it is clear that they remained at the theory stage.

3. Methodology and Proposed Method

In this section, a comprehensive look at blockchain steganography methods is carried out. It is clear from the presented materials that there are many shortcomings in both blockchain and stenography. Hence, the proposed OTA algorithm is presented as an alternative method that solves many current outstanding problems.

3.1. Steganography: An Overview

Steganography is studied in four main domains. These are the spatial domain, the transform domain, the spread spectrum domain, and the model-based domain. The data bits to be hidden in the spatial domain are directly hidden in the cover image. The Least Significant Bit (LSB) [30] method is a widely used and known algorithm in this field. The use of the LSB algorithm is simple, fast, and it is very difficult to detect visually without statistical methods. However, in case of a change as a result of any effect on the multimedia where the data is hidden, it becomes impossible to access the hidden data. Pixel Value Differencing (PVD) and Binary Pattern Complexity (BPC) are a few other methods used in the spatial domain.

The data to be hidden in the transform domain is hidden in the cover multimedia using transposition. The most familiar methods are Discrete Cosine Transform (DCT) [31,32], Discrete Haar Wavelet Transform (DWT) [33], and Discrete Fourier Transform (DFT). Considering that the cover used in DCT will be an image, it divides the image into 8×8 blocks. In these blocks, sensitive areas to hide data are determined, and then steganography takes place. Considering that the cover used in DWT will be an image, the cover image is divided into four sub-bands. These sub-bands are high–high (HH), high–low (HL), low–high (LH), and low–low (LL). Data hiding is preferred in the LL band. Regardless of the data size hidden using the DWT algorithm, when you divide the cover multimedia into sub-bands and then combine them, the multimedia you get will not have the same structure. The DWT algorithm causes permanent corruption on the cover multimedia, but this situation does not affect the stego-data, which is hidden in the LL band. In DFT, discrete-time signals are converted to discrete frequencies. However, discrete-time is used and converted to continuous frequency. DFT transforms a vector list of instances of a function into a finite list of coefficients ordered by frequency. Discrete Fourier transform series is a high-speed algorithm. As a result of the application of DFT on computers, fast Fourier transform is also called FFT.

Spread spectrum image steganography is a process of storing an encrypted message as a Gaussian noise in a cover image. This method relies on the fact that low noise power levels cause little image degradation and therefore it is undetectable by the human eye. Even if there is some data loss in the bands, it is possible to reach the secret data by using the data left behind. As long as all cover multimedia is not removed, access to secret data can be achieved. For this reason, this technique is preferred in military applications.

In a model-based domain, cover multimedia is divided into two parts; only the second of these parts is for hiding data. While performing steganography, the statistical properties of cover multimedia are not changed. As the size of the data hidden by this method increases, the detection rate using various stego-analysis methods is much lower than in the transform domain. For this reason, it is preferred in steganography studies where large amounts of data are hidden. However, data hiding and extracting from stego-multimedia in this domain take much more time than the examples seen in other domains [34].

There are requirements that steganography must meet at a successful rate in order to be considered: imperceptibility (undetectability), security, payload capacity, robustness. Imperceptibility is one of the vital requirements in steganography. Imperceptibility is the inability to detect secret data hidden in cover multimedia using various steganography techniques by statistical or visual analysis. After applying steganography, the smaller the difference between cover multimedia and stego-multimedia, the higher the imperceptibility. Histogram, peak signal-noise ratio, mean squared error, structural similarity index measure, and similar quality metrics are all used to measure imperceptibility.

Security means that hidden data cannot be obtained if the stego-multimedia is detected using steganalysis methods. There are methods in which various encryption algorithms are used to provide security, such as encryption of stego-data or encryption of stego-multimedia. In addition, the provision of a secured communication channel is essential to protect against steganalysis methods and increase security.

Payload capacity refers to the maximum data that can be hidden in cover multimedia without affecting imperceptibility and security. Successful steganography aims to use the minimum amount of cover multimedia while obtaining the maximum payload. Embedding rate is the ratio of used secret data used in cover multimedia obtained at a high rate.

Robustness means that the data hidden using any steganography technique can be obtained from stego-multimedia without any loss after compression, scaling, resizing, rotation, and similar effects [35,36].

The mediums in which steganography techniques are applied is important in digital steganography [37]. Steganography techniques are applied in mediums such as text, image, network, audio, and video. In addition to these mediums, blockchain should be added to the literature. In blockchain steganography, a new hiding method emerges as a steganography technique. It should be noted that blockchain steganography is different from network steganography. As seen in the literature review section, blockchain steganography studies are based on applying conventional methods differently and assuming novel methods. For this reason, the blockchain medium in digital steganography is an innovation that should be considered as a separate topic.

The purpose of steganalysis methods is to detect steganographic communication using various technological possibilities. Although steganography is an old subject of study, studies on steganalysis methods started at the end of the 20th century due to the opportunities provided by modern technology. Steganalysis methods developed for the detection of widely used steganography techniques offer successful results. Such steganalysis methods are called targeted methods. A general definition of steganalysis methods makes determinations through statistical analysis (such as the pairs of values method) [38]. The artificial intelligence-assisted steganalysis [20] method has been used successfully due to the availability of advanced computer hardware and advances in deep learning techniques.

As can be seen, there is a high demand for stronger methods against steganalysis to maintain security and confidentiality at a high level. Because, as with any steganography technique performed on cover multimedia, data hiding will be at risk and become detectable at some stage. The most basic condition to be met is that cover multimedia is not available publicly online. It should not leave an accessible trace by using new steganography methods developed over private platforms. For this reason, blockchain technology offers an excellent opportunity to provide the private platform needed.

3.2. Blockchain: An Overview

Blockchain technology is the second technological development with a similar effect on our lives after internet technology, and its impact continues to increase day by day. Blockchain technology has been introduced as the creative power of Bitcoin crypto money in response to the need for a system with a high level of transparency and anonymity to prevent misleading information from central authorities. Blockchain technology can be described as a distributed database. Similarly, it is also called distributed ledger technology. Because the blocks that make up the blockchain are accepted by the nodes that make up the system to record the transactions performed, and the current transaction records are available in all nodes, distributed ledger technology is ascribed. As the name suggests, all transactions carried out in the blockchain system are recorded and stored in blocks, just like the pages of a ledger. In this context, the blockchain system works like a ledger. However, this ledger is not stored in a single location but in all nodes that make up the blockchain. This way, targeting the database cannot be a realistic goal. As a result of this feature, blockchain systems have a high level of data security [39].

In the case of Bitcoin, it is the nodes that make up the system transfer crypto money between each other. The Bitcoin blockchain platform is a public blockchain. In other words, anyone who wants to join the system can become a participant as a node and examine all the transactions that have taken place since the first block. In the Bitcoin blockchain, the nodes are anonymous; that is, the affiliation of the nodes is unknown. Each node has a wallet, and this wallet has two keys. While the public key is the publicly known address of the node, the private key is the private key of the node owner to access the system. If the private key is lost, access to the system is not possible. Nodes can send Bitcoins to each other peer-to-peer through these wallets without the need for any third party. In this context, blockchain systems have a decentralized structure [40].

The most basic unit that makes up the blockchain is the blocks. Except for the first block, the genesis block, all blocks have two hash function values. One of them is the previous block's hash value, and the other is the hash value produced in its block. Hash functions are cryptological algorithms that work unidirectionally and give you fixed results. Today, secure hash algorithm SHA256 is a widely used algorithm that produces 256-bit values. It will be seen that the hash value changes as a result of the slightest change in the data used in the calculation of the hash value. This feature ensures that the transaction records recorded in the blockchain cannot be changed, thus providing a high level of security. The secure system, obtained by connecting the blocks using hash values, brings a tamper-proof feature to the blockchain.

The Bitcoin blockchain database is accessible to the public, expressed in the Bitcoin example, and is not a condition that must be used in all blockchain solutions. Public blockchains are generally preferred in applications where the participation of cryptocurrencies or the entire society is expected. On the other hand, private blockchains [41] are frequently preferred in cases where privacy and access are desired to be limited. Blockchains, which are designed to be integrated into hospital systems, are the preferred models of the digital services offered by states to their citizens and are implemented with blockchain technology. Here, access to the system is authenticated, and it is determined beforehand who can see how much data and what actions they can take. The use of private blockchains will have significant advantages in studies requiring data security and blockchain technology [42].

In blockchain systems, those who record data in blocks are called miners. These miners provide the necessary processing power that the system needs and receive coins as a reward to meet the necessary conditions and be entitled to create a block. This reward system is an incentive feature in many blockchain systems. There are consensus algorithms used to write the information to be recorded in blocks in blockchains. Consensus algorithms are used in all crypto money systems and such algorithms are Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT). Each consensus algorithm has some negative features associated with it. For example, while the PoW algorithm requires high processing power and causes high energy consumption, the PoS algorithm gives more rewards to wallets holding a large amount of cryptocurrencies and allocates the right to create the block among these wallets. While solutions to these problems are still being sought, the point to be considered is that the consensus algorithm to be used to develop the proposed blockchain is chosen very carefully. It is possible to create system-specific consensus algorithms [43]. In this context, today, many new consensus algorithms are being developed that are environmentally friendly, fair reward sharing, and specifically to solve the problems they encounter, e.g., PoW-BC [44]. However, incorrectly chosen consensus algorithms that are not suitable for the developed blockchain system cause serious problems.

Innovative methods are being developed to solve new cases such as Hyperledger, NEO; Helium is a new application platform designed to realize the use of blockchain technology outside of financial solutions [29]. Hence, while introducing blockchain systems, on-chain and off-chain concepts are necessary. The on-chain concept refers to recording all transaction information in blockchain blocks, and this logic is used in Bitcoin, Ethereum,

and many other crypto money systems. On the other hand, off-chain is a method used in cases that are too large to be recorded on the blockchain or that need to be modified or deleted in the future.

Another concept that needs to be expressed is smart contracts. The concept of a smart contract was proposed by Nick Szabo [45]. Smart contracts are small pieces of code that enable a specified action to be performed for a specific situation. Blockchain taxonomy is shared in Figure 1.

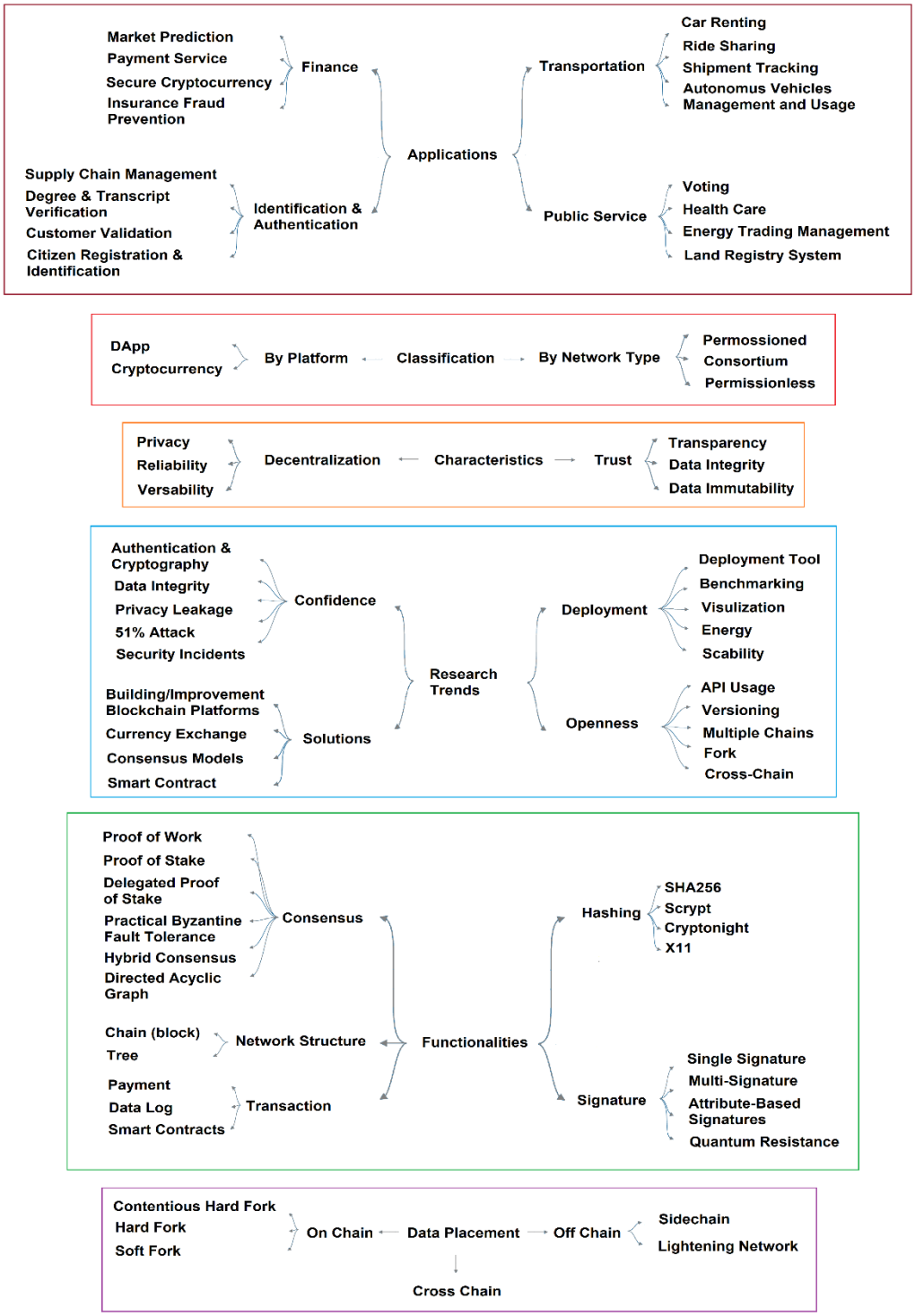

Figure 1. Blockchain taxonomy.

The transaction volume and speed of blockchain technology are not sufficient compared to the systems used today. However, improvement works in this area are carried out by the community. Another point to be noted is the costs. The usage costs of platforms that enable us to develop private blockchain solutions such as Hyperledger are at the levels that require monthly payments starting from USD 1000 in 2018 to USD 6000. Again, considering the Bitcoin prices in 2018, the cost required for a transaction is USD 1.30, and on the Ethereum platform, it is USD $0.30 [46]. For this reason, the usage costs of blockchain platforms are far from being reasonable due to the rise in cryptocurrencies [47,48].

3.3. Proposed Ozyavas–Takaoglu–Ajlouni (OTA) Algorithm

The OTA algorithm is a private blockchain system developed for steganographic communication. It has been developed from scratch using the Java and JavaScript programming languages. Because it is a private blockchain system, access to the OTA system is subject to permission. Initially, 50 OTA coins are allocated to the wallets of the nodes that have been granted access. The cost of each transaction sending in the system has been determined and fixed at 1 OTA coin. The proposed algorithm consists of two stages. The first stage is the steganography process, and the second stage is sending the stego-data by the private OTA-chain blockchain system. Preparations are being made by the Istanbul Aydın University Blockchain Application and Research Center to ensure the worldwide use of the developed OTA algorithm. The back-end part of the OTA algorithm has been implemented. The OTA-chain platform will be accessed when its front-end is accomplished.

3.3.1. OTA-Steganography Algorithm

In the proposed OTA-steganography algorithm, the multimedia selected as covers are stored on a private server. The URLs of these multimedia are referred to and stored in the blocks in the OTA-chain. This way, when the cover multimedia is sent using the public channel, various unintentional distortions in the cover multimedia can be detected and corrected. Because the OTA-steganography algorithm does not hide any data in the cover multimedia image, it cannot be detected by any steganalysis method. Therefore, it differs from conventional steganography and has its own novel structure. The plaintext data is divided into 2,3,4, etc., number of bits depending on the chunk size to be used. Whatever the choice of division, a sequential search for plaintext data bit patterns will be performed in the cover multimedia file for matching bit pieces. Once the algorithm finds a match, the matching pieces starting bit number, or index, in the cover multimedia is saved. The search continues for remaining plaintext data bit pieces from where the last successful search in the cover multimedia ended. If a search for a piece of the plaintext reaches the end of the cover multimedia before it finds the matching bit pattern, the search continues at the beginning of the cover multimedia file, hence making the process cyclic. When all bit patterns in the plaintext data in the cover multimedia file are found, the algorithm places the saved indices in an array. The array containing the indices is called the "address array" in the rest of the discussion. This array is divided into 1 kilobyte (kB) arrays, and each 1 kB of stego-data corresponds to 1 transaction in the OTA-chain. In Figure 2, the architecture of the OTA-steganography algorithm is shared.

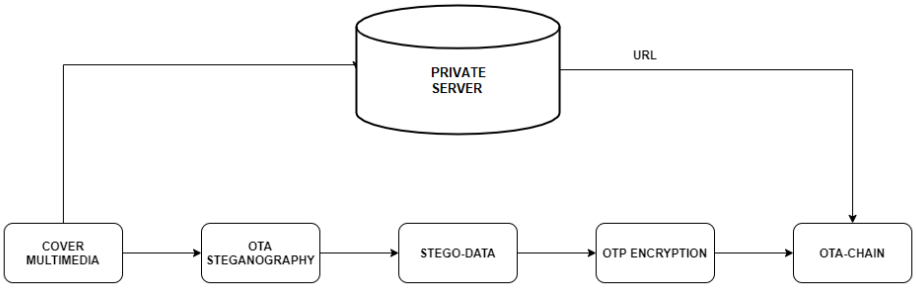

Figure 2. Architecture of OTA Steganography.

The probability of not finding a bit pattern of length n in a cover multimedia of length m where m > n is computed using Markov chains. The details of different length bit patterns, cover multimedia length, and their probabilities are shown in Table 1. Eight-bit divisions of the message are well suited because 1 kB of data requires 1 kB of address array, which is the size of a transaction in the private blockchain. It can be seen in Table 1 that the probability of not finding any 8-bit pattern in a small size cover multimedia is extremely small. That is, the probability of finding any 8-bit pattern in cover multimedia of size above 256 bytes is almost 100%.

Table 1. Probability of finding n-bit pattern in an m-bit cover multimedia.

	128 Byte	256 Byte	512 Byte	1 kB	4 kB
4-bit pattern	~100%	~100%	~100%	~100%	~100%
6-bit pattern	99.99%	~100%	~100%	~100%	~100%
8-bit pattern	98.34%	99.97%	99.99%	~100%	~100%
10-bit pattern	63.30%	86.62%	98.22%	99.96%	~100%

While the OTA-steganography algorithm processes the cover multimedia, indices of 2, 3, and 4 bit pieces of the plaintext data are saved for performance comparison. Using bigger chunks will result in a shorter address array, but it will take more search time for the address array creation. Stego-data, the address array in this case, obtained from the OTA-steganography algorithm is encrypted using the One-Time-Pad (OTP) algorithm [2]. The OTP key can be shared using any method because the OTA-chain does not pose a risk if the key is in the hands of undesirable parties in the public channel because it is in a private OTA blockchain. Even though the proposed system is designed for small-sized messages, data bigger than the cover multimedia file can be transformed into an address array because of the cyclic nature of the algorithm. Figure 2 illustrates the block diagram of the OTA-steganography algorithm.

The proposed OTA-steganography algorithm achieves an almost unlimited payload capacity by using a single cover multimedia with its precise marking and indexing technique.

The pseudocode of the OTA-steganography algorithm is represented in Algorithm 1. A refers to the cover multimedia, B refers to the secret data, and C refers to the address arrays. Ciphered Secret Data (CSD) is the encrypted form of the most optimal C arrays obtained as a result of applying the OTA algorithm on secret data.

The method of recovering the secret data hidden by the OTA-steganography algorithm is presented in Algorithm 2, where A represents the multimedia obtained from the URL, K is the key, and Ci is the information of how many bits the plaintext is divided into, that is, pieces. CSD refers to the encrypted steganographic information received from the OTA-chain. The cover multimedia obtained from the server is used together with the marking addresses obtained by applying a reverse OTP algorithm using the key and CSD data. The addresses in the C array are read one by one, found in the A cover multimedia, and written into the B array. When the algorithm completes its work, the secret data hidden by the OTA-steganography algorithm is fully recovered.

Because the OTA-steganography algorithm uses the cover multimedia bits' addresses to represent the bits of the secret data, it does not cause any deterioration to the multimedia file. Thus, all steganalysis techniques used today become useless. Keeping the used cover multimedia on a private server is of great importance for the OTA-steganography algorithm because, theoretically, any corruption in the public channel and on the cover multimedia will cause some changes in the plain text. For this reason, it has been decided that using a server for cover multimedia in the OTA-steganography algorithm is a safer method. In addition, testing shows the use of public channels detected no change in the cover multimedia.

Algorithm 1. OTA-Steganography Algorithm

let A = {A_1,A_2,A_3,...,A_n}
let B = {B_1,B_2,B_3,...,B_n}
upload the cover multimedia to the server and get URL
//for 2 bits marking
let C_{tb} = { C_{tb1},C_{tb2},C_{tb3},...,C_{tbn} } **then**
C_{tb} = C_{tb1} **then**
if B ≠ {} **then**
    for A and B **do**
        if A_n == B_n **do**
            add A_n.location to C_{tb} **then**
            erase B_n from B
            if C_{tb1}.lenght >= 1024 **then**
                let C_{tb} = C_{tbn+1}
            end if
        end if
    end for
end if
//for 3 bits marking
let C_{thb} = { C_{thb1},C_{thb2},C_{thb3},...,C_{thbn} } **then**
C_{thb} = C_{thb1} **then**
if B ≠ {} **then**
    for A and B **do**
        if A_n == B_n **do**
            add An.location to Cthb **then**
            erase Bn **from** B
            if Cthb.lenght >= 1024 **then**
                let C_{thb} = C_{thb1+1}
            end if
        end if
    end for
end if
//for 4 bits marking
let C_{fb} = C_{fb1},C_{fb2},C_{fb3},...,C_{fbn} **then**
C_{fb} = C_{fb1} **then**
if B ≠ {} **then**
    for A and B **do**
        if A_n == B_n **do**
            add A_n.location to C_{fb} **then**
            erase B_n from B
            if C_{fb}.lenght >= 1024 **then**
                let C_{fb} = C_{fb1+1}
            end if
        end if
    end for
end if
let C = {}
select min.lenght (C_{tb},C_{thb},C_{fb}) —>C **then**
let C_i = selected (C_{tb},C_{thb},C_{fb}) information
//Marking part will continue to the desired bits number. In our study it's 10
//One Time Pad process
let K
let CSD
generate K size of C.lenght **then**
CSD = K ⊕ C
return CSD, K, C_i, URL

Algorithm 2. Inverse OTA-Steganography Algorithm

1: **get** A cover multimedia from server
2: **get** K and Ci from sender
3: **get** CSD from OTA-chain
4: **let** B = { B_1,B_2,B_3,...,B_n }
5: C = CSD $\oplus$ K **then**
//consider C_i bit information for data extracting process
6: **for** C **do**
7: **go** $A_{c.address}$ **then**
8: $B_n = A_{c.address}$
9: **end for**
10: **return** B

3.3.2. OTA-Chain Algorithm

The OTA-chain algorithm has been specially developed to meet steganographic needs. Nodes in the OTA-chain system containing steganographic information can securely communicate with each other. Platforms such as Bitcoin, Ethereum blockchain, or the Hyperledger platform have not been used. The reason for this is to keep the system costs lower, as stated in the previous sections. Because the OTA-chain system works using OTA coin, an OTA coin will be sent to the receiver together with stego-data, and the coin for the receiver's wallet functions as a reminder with a warning message to the user. That is, coin sending works like a ring mechanism that informs the receiver.

Most importantly, the OTA coin is distributed free of charge to the nodes that have been granted access so that the system cost is limited only by the hardware processing power provided by the nodes. Developing the OTA-chain algorithm from scratch allowed many needed features to be added to the system at the beginning. The block structure of the proposed system that meets steganographic needs contains sender address, receiver address, timestamp, last hash, hash, nonce, difficulty, URL, and data.

- Sender and Receiver Addresses: 256-bit unique addresses of the sending and receiving nodes in the blockchain system.
- Timestamp: This is the date and time information created when a transaction is performed.
- LastHash: In the blockchain, the hash value of the last block created, excluding the genesis block, is called lasthash. It is a 256-bit value, calculated with the SHA256 algorithm.
- Hash: 256-bit value generated using the SHA256 encryption algorithm. Each block has its own hash value and lasthash, which is the previous block's hash value.
- Nonce: A 32-bit value randomly generated when creating the block, which stands for Number Only Used Once. The Nonce value is used for the operation of the reward system in our PoW algorithm, in which the miners in the system participate.
- Difficulty: The ease of resolution of the PoW algorithm is used to win the block writing right, and the reward is called difficulty. The difficulty level is automatically increased or decreased according to the status of participation in the system.
- URL: In the proposed OTA algorithm, cover multimedia are saved in the server for system security, and its URL is kept in the OTA-chain block, which the receiver uses to reach the cover media.
- Data: This is the field where the OTA coin information sent on the OTA-chain is kept.
- StegoData: This is the 1 kB address array OTP-ciphered stego-data sent over to and stored in blocks of OTA-chain.

The OTA-chain block structure is illustrated in Figure 3.

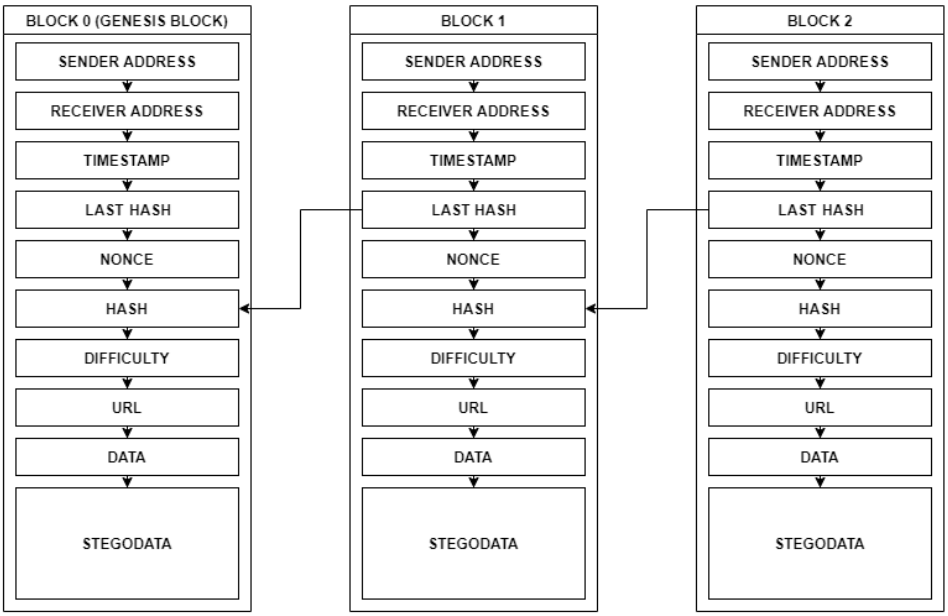

Figure 3. OTA-chain block structure.

The OTA-chain algorithm proposes a private blockchain system. In this case, undesirable parties who do not have permission to access the system do not have the opportunity to examine the transactions. The transmitted stego-data is encrypted with the OTP algorithm and then recorded in blocks of the system in order to prevent the nodes that are granted access to the system from falling into the hands of undesirable parties or from manipulating the system by a node (insider attack). Nodes have the opportunity to examine only those transactions that take place in the OTA-chain system.

The Proof-of-Work algorithm is used as the consensus algorithm in the proposed algorithm. The nodes that make up the system also work as miners. Nodes that get block writing rights are rewarded with 50 OTA coins. Additionally, the minimum transaction price to be performed on the OTA-chain has been determined as 1 OTA coin. Each up-to 1 kB-size transaction uses exactly 1 OTA coin. Stego-data used in the OTA-chain are all 1 kB-CSD-encrypted array produced in the OTA-steganography stage. Thus, the encrypted data is divided into 1 kB blocks, and the number of transactions is how many 1 kB blocks this confidential data contains.

The OTA-chain algorithm is an on-chain blockchain system. The information of the data used in the system is recorded in OTA-chain blocks. Picture matrices are not hidden in system blocks, as seen in similar studies, and this saves time and processing power. Additionally, the proposed system does not suffer from the cost caused by the ready-made platforms used in previous studies shown in the literature. In the OTA-chain system, the URL address of the cover multimedia that the buyer needs are securely shared with encrypted stego-data. The block diagram expressing the OTA-steganography and OTA-chain architecture of the proposed OTA algorithm is illustrated in Figure 4.

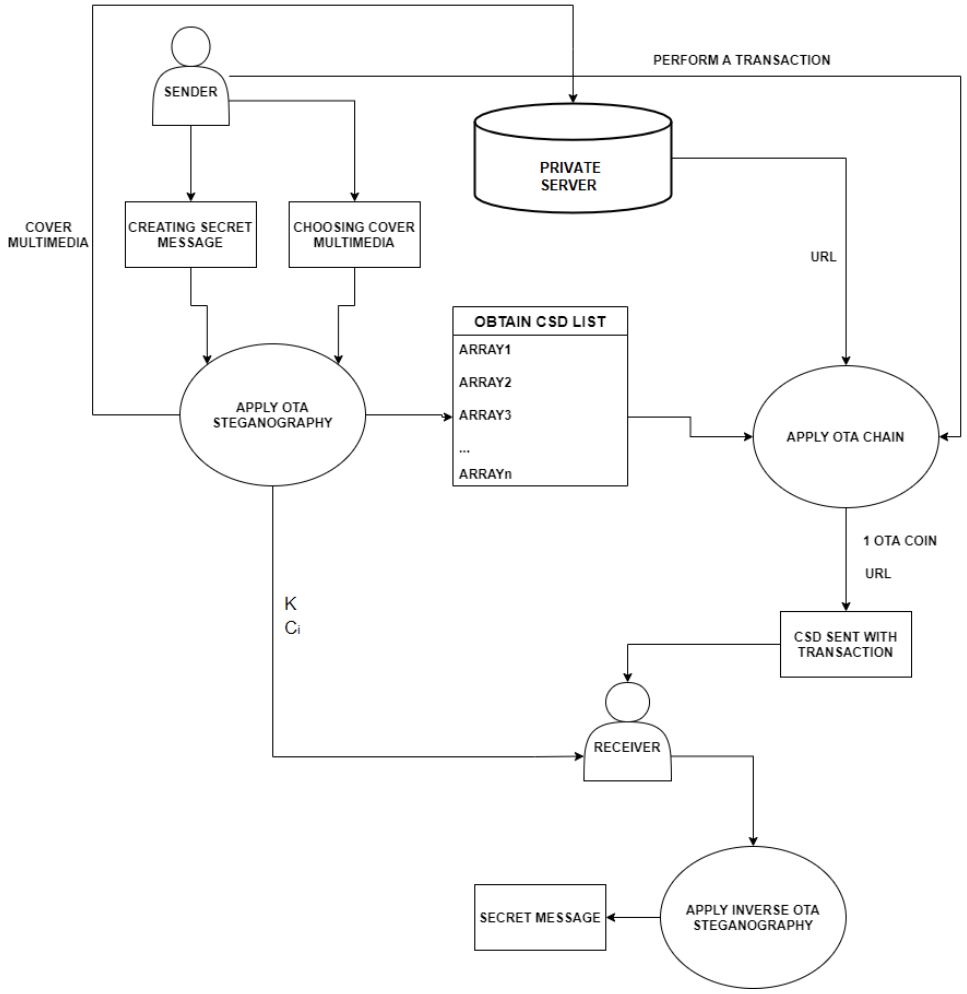

Figure 4. Structure of OTA Algorithm.

4. Results and Discussion

Tests were carried out using an Intel Core i7 7700 HQ processor and 8 GB Ram computer. The OTA-steganography algorithm was developed with the Java programming language, while the backend component of the OTA-chain algorithm was coded with the JavaScript programming language. The coded OTA-chain system was tested using Git Bash and Postman applications.

A total of 32 images were used as cover multimedia during the testing of the proposed algorithm. The testing selected cover images are 256 × 256 pixels in size, and pictures are assigned names in the range of CI-1 through CI-32. These cover images were selected from the USC-SIPI Image Database Version 6. The selected images are illustrated in Figure 5. The data to be hidden is determined as 1 kB, 5 kB, 10 kB, and 20 kB.

An example data of 1 kB is shared in Figure 6. However, big data sizes for steganographic communication such as 5 kB, 10 kB, and 20 kB were used to test the capabilities of the proposed OTA algorithm. The tests show that any data can be used because the system will perform exactly the same regardless of the data size. The type and size of cover multimedia used is of no importance to our algorithm because the first 256 × 256 byte section is selected for the marking/indexing process.

The OTA-steganography and OTA-chain algorithms, which are the two sub-titles of the OTA algorithm, are shared under the analysis Sections 4.1 and 4.2.

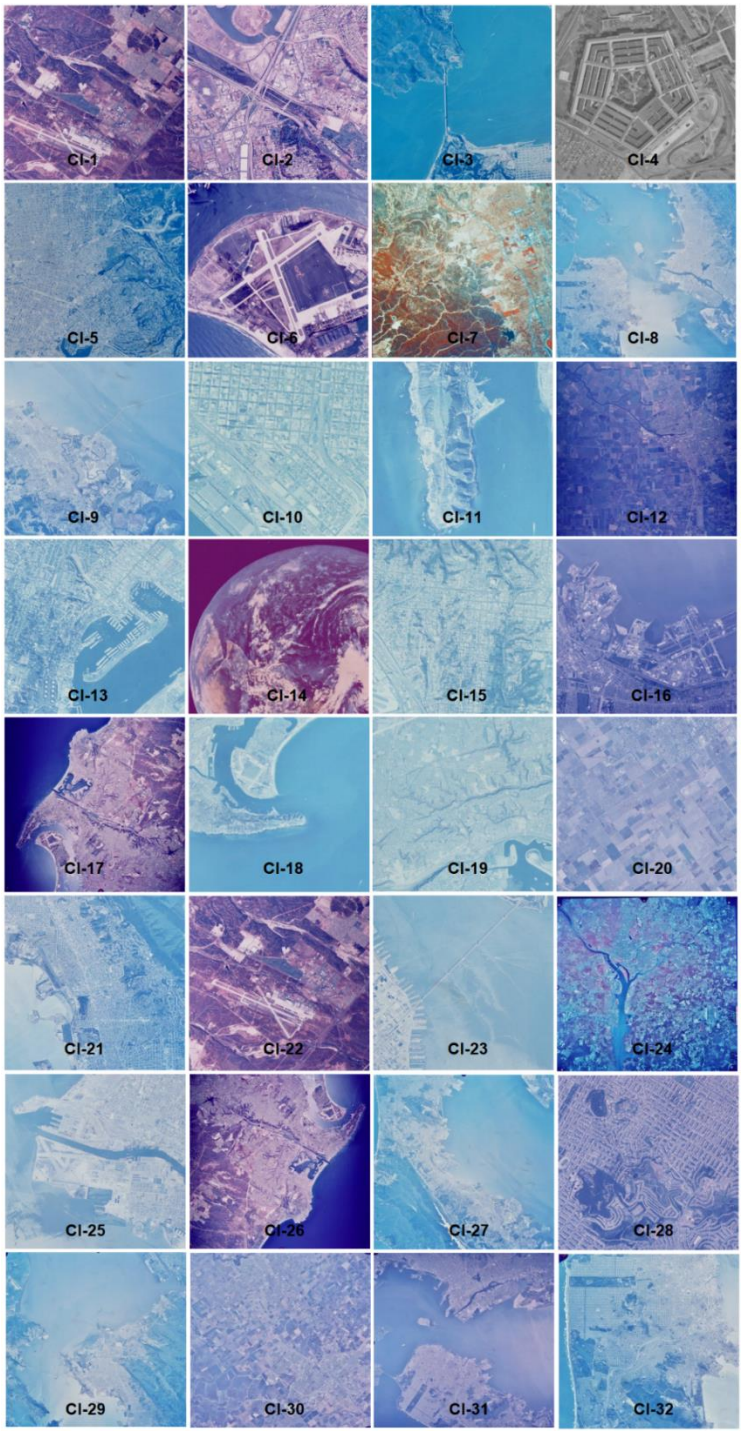

Figure 5. USC-SIPI Cover Images.

The first recorded uses of steganography can be traced back to 440 BC in Greece, when Herodotus mentions two examples in his Histories. Histiaeus sent a message to his vassal, Aristagoras, by shaving the head of his most trusted servant, marking the message onto his scalp, then sending him on his way once his hair had regrown with the instruction, When thou art come to Miletus, bid Aristagoras shave thy head, and look thereon. Additionally, Demaratus sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. Wax tablets were in common use then as reusable writing surfaces sometimes used for shorthand. In his work Polygraphiae Johannes Trithemius developed his socalled AveMariaCipher that can hide information in a Latin praise of God. Auctor Sapientissimus Conseruans Angelica Deferat Nobis Charitas Potentissimi Creatoris for example contains the concealed word VICIPEDIA.

Figure 6. Example of 1 KB Secret Data.

4.1. OTA-Steganography Results

Table 2 shows the results of applying the OTA-steganography algorithm with 1 kB, 5 kB, 10 kB, and 20 kB secret data and cover image number 1 (256 × 256 pixels). The OTA algorithm results show the total array size of the marked data addresses, the number of arrays used to hide the data, and the time required. The same test was applied to the remaining 31 images. The results prove the algorithm suitability for the proposed task (complete test results can be obtained by contacting the author directly).

Table 2. OTA-Steganography CI-1 Results.

Embeded Data Size	**1 kB**					**5 kB**					**10 kB**					**20 kB**				
Bit Block Size	2 Bits	4 Bits	6 Bits	8 Bits	10 Bits	2 Bits	4 Bits	6 Bits	8 Bits	10 Bits	2 Bits	4 Bits	6 Bits	8 Bits	10 Bits	2 Bits	4 Bits	6 Bits	8 Bits	10 Bits
Encoding time (ms)	3	2	6	22	6645	6	7	24	4895	28,073	11	14	28	69	30,330	26	25	45	89	30,217
Array size	3916	1958	1306	979	784	19,580	9790	6527	4895	3916	39,160	19,580	13,054	9790	7832	80,524	40,262	26,842	20,131	16,105
No of arrays required	4	2	2	1	1	20	10	7	5	4	39	20	13	10	8	79	40	27	20	16

As seen from Table 2, the cover images used have no effect on the total array size and the number of arrays created as a result of the application of the OTA-steganography algorithm. This is due to the marking/indexing process performed on an array of 256 × 256 bytes, as the results show the cover images differ only in the time spent in the marking process. Table 2 results reveal that the differences in the bit sequences of the cover images do not cause a big difference in time, so that the cover multimedia selected in steganographic studies using the OTA-steganography algorithm does not have a significant effect on the success of the OTA algorithm.

4.2. OTA Blockchain Results

The cover image, whose URL address is stored in the transaction data, is used by the OTA-steganography algorithm, and the address array obtained by marking 1 KB of plaintext data using 8-bit blocks is encrypted with OTP and then transmitted to the receiver using OTA-chain, as shown in Figure 7. Single OTA-chain coin was spent in the realization of this transaction. The transaction took place instantly in the test environment, and the sending node was rewarded with 50 OTA coins for gaining the right to write blocks. The address arrays created by the OTA-steganography algorithm for 10-bit marking for different sizes of plaintext data can be sent inside transactions easily because a 50 OTA coins is allocated to the accounts of the nodes when they join the system. The continuing steganographic communication within the system ensures that OTA coins will change hands so that even if the nodes do not receive the miner reward, they will have enough coins to trade in the system. Therefore, the OTA-chain algorithm provides a sustainable blockchain steganography communication.

Figure 7. Example of OTA-Chain Transaction.

The OTA-chain algorithm was developed with decentralized, scalability, security, and cost in mind. Even though the proposed system may require a considerable amount of time for very large data, it does not suffer in terms of scalability because steganographic communication will only use relatively small size data. Additionally, due to the difficulty level of the PoW algorithm in low transaction volume systems, energy consumption will be kept at a minimum level. Additionally, because the system is a private blockchain, attacks common to public blockchains are prevented. Encrypting the transmitted information with the OTA encryption algorithm in order to avoid insider attacks has elevated the internal security of the system to the next level. Because the OTA-chain private blockchain system uses its own coin and distributes it free of charge to the nodes with access rights, system costs are limited in that users required only to record transactions as a miner for their hardware.

The theory of the proposed OTA-chain algorithm has been put into practice. After the front-end work of the system is completed, it will be shared with the public. The OTA-chain system ensures complete anonymity. Transactions performed in the system can be followed, but it is not possible to track down the users. With the proposed system, real-time data access is provided. It is resistant to all kinds of steganalysis methods and has a tamper-proof structure. The system is closed to the intervention of third parties.

4.3. General Analysis of OTA Algorithm

The OTA algorithm is a novel blockchain steganography algorithm. Its design takes into consideration the new techniques offered by blockchain technology and is not based on traditional steganography techniques. The proposed algorithm provides enhancements on hiding capacity (payload capacity), imperceptibility, security, and robustness, which are emphasized in steganography studies. None of the deficiencies seen in the studies expressed in the literature review are applicable to the OTA algorithm. For example, the payload capacity, which Sarkar et al. [22] tried to increase in the proposed study, has been made unlimited. Secret data of any size can be hidden using a single cover multimedia without causing any deterioration on the cover multimedia.

In the study proposed by Mohsin et al. [23], COVID19 data, including high-resolution images, are transmitted over the blockchain system. Unlike this system, where the blockchain system is burdened with storing high volumes of data, the OTA algorithm transmits only an encrypted address array using only 1 KB data, with only indictors of the actual data, not the actual data itself.

Basuki and Rosiyadi [24], on the other hand, used the LSB method within their proposed Ethereum platform and introduced it as transaction steganography. Although the study is designed much more robustly than its counterparts, it remains weak at hiding capacity due to the use of the traditional steganography technique. In addition, because the Ethereum system is used, each transaction costs more as the value of Ether increases. The OTA algorithm is superior in terms of hiding capacity and cost.

Partala's [25] theoretically proposed work can send 1 byte of stego-data requiring more than one hour to accomplish its task. In terms of speed, the OTA algorithm performs better.

Although the RDHEI algorithm proposed by Horng et al. [26] is difficult to implement in real life, it offers 0.8 bpp embedding rate success. In the OTA algorithm, the embedding rate is 100%.

Xu et al. [27] aimed to transmit steganographic information using the existing public blockchains. However, the hardware requirements to be a miner in public blockchains such as Bitcoin and Ethereum and the information that can be inserted in a block specified in the genesis block are limitations in such a system. In this context, the OTA algorithm overcomes the public blockchain handicap faced by Xu et al. [27] and offers a platform where stego-data can be recorded without any problems because of its initial design.

Giron et al. [29], on the other hand, proposed a staganalysis method to detect blockchain steganography. As stated in their studies, there is no steganographic communication they

can detect. Because of the private blockchain used by the OTA algorithm, the steganalysis methods they suggested do not work because they cannot access it.

The blockchain leg of the algorithm ensures that the system is decentralized, anonymous, and tamper-proof. In addition, because the author developed all the coding required by the OTA algorithm, the algorithm's future improvement can easily be implemented, resulting in zero system cost. Because the OTA algorithm is proposed to address a specific need, it is likely that blockchain will not receive the high attention that many finance applications have. This has a positive effect on the system's scalability issue because the consensus algorithm works without difficulty. In addition, the weaknesses to be encountered during the completion of the front-end studies of the system and the public trial of the system will be carefully examined, and the improvement processes will be carried out continuously.

The proposed system moves away from traditional steganography. It does not embed the secret data in the cover multimedia, thus causing no degradation in the cover multimedia, but uses blockchain blocks as its medium to store the secret data. It also utilizes the proposed private OTA blockchain as an additional layer of security while storing the encrypted address array as transactions. The OTP encryption applied to the address array that contains the indices from the cover multimedia encoding the secret message aims to prevent insider attacks. Private blockchain system integration also ensures that the proposed system is decentralized, anonymous, and tamper-proof. In addition, any weaknesses encountered during the implementation of the front-end of the system and the public trial will be carefully examined, and any required improvement processes will be carried out continuously.

5. Conclusions

The OTA algorithm is proposed as a novel method for blockchain steganography. It eliminates the deficiencies faced by traditional steganography with blockchain technology. In this context, novel OTA-steganography and an OTA-chain algorithm are presented. The proposed algorithms were tested with real data. The results show that the algorithm performed with a very low system cost and is resistant to all steganalysis methods, with no information hiding capacity limit, and with a high level of security. When compared with the studies in the literature, it is clear that the proposed method is positively different and able to overcome issues such as hiding capacity, resilience to steganalysis, cost of application, and the hard-to-realize goals of the previous studies. In the future, the authors intend to develop and introduce smart contracts in the OTA algorithm so that the system will react to predefined conditions. There is also a need for studies on the development of applicable steganography methods using public blockchain systems.

Author Contributions: M.T. is the main researcher in this article and implemented the code and carried out all the required research testing, background review, and the preparation of the original and final manuscript; N.A. is the principle investigator; he provided the basic methodology and the supervised the implementation and verified the results; A.Ö. provided the necessary coding support and technical support need by the team; A.A. verified the testing data and supervised the drafting of the first version of the manuscript; and B.A., verified the methodology and supervised the technical implementation. All the authors contributed to the preparation of the final manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: This study does not include any testing of humans or animals of any form.

Informed Consent Statement: Not applicable.

Data Availability Statement: There are no supporting data or reports related to this study.

Acknowledgments: We would like to thank Istanbul Aydın University Blockchain Application and Research Center for its support in the development of the OTA algorithm. The authors would like to thank the Arab Open University, Saudi Arabia, for supporting this study.

Conflicts of Interest: The authors declare no conflict of interest. The research received no funding and hence no funders had any role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Subramanian, N.; Elharrouss, O.; Al-Maadeed, S.; Bouridane, A. Image Steganography: A Review of the Recent Advances. *IEEE Access* **2021**, *9*, 23409–23423. [CrossRef]
2. Setiadi, D.R.I.M.; Rachmawanto, E.H.; Sari, C.A. Secure Image Steganography Algorithm Based on DCT with OTP Encryption. *J. Appl. Intell. Syst.* **2017**, *2*, 1–11. [CrossRef]
3. Pandey, J.; Joshi, K.; Jangra, M.; Sain, M. Pixel Indicator Steganography Technique with Enhanced Capacity for RGB Images. In Proceedings of the 2019 International Conference on Intelligent Computing and Control Systems (ICCS), Madurai, India, 15–17 May 2019; pp. 738–743. [CrossRef]
4. Islam, M.A.; Riad, M.A.A.K.; Pias, T.S. Enhancing Security of Image Steganography Using Visual Cryptography. In Proceedings of the ICREST 2021—2nd International Conference on Robotics, Electrical and Signal Processing Techniques, Khaka, Bangladesh, 5–7 January 2021; pp. 694–698. [CrossRef]
5. Reinel, T.S.; Brayan, A.A.H.; Alejandro, B.O.M.; Alejandro, M.R.; Daniel, A.G.; Alejandro, A.G.J.; Buenaventura, B.J.A.; Simon, O.A.; Gustavo, I.; Raul, R.P. GBRAS-Net: A Convolutional Neural Network Architecture for Spatial Image Steganalysis. *IEEE Access* **2021**, *9*, 14340–14350. [CrossRef]
6. Su, W.; Ni, J.; Hu, X.; Fridrich, J. Image Steganography with Symmetric Embedding Using Gaussian Markov Random Field Model. *IEEE Trans. Circuits Syst. Video Technol.* **2021**, *31*, 1001–1015. [CrossRef]
7. Zhang, L.; Zhang, Z.; Wang, W.; Jin, Z.; Su, Y.; Chen, H. Research on a Covert Communication Model Realized by Using Smart Contracts in Blockchain Environment. *IEEE Syst. J.* **2021**, 1–12. [CrossRef]
8. Latypov, R.; Stolov, E. A New Watermarking Method to Protect Blockchain Records Comprising Small Graphic Files. In Proceedings of the 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 1–3 July 2019; pp. 668–671. [CrossRef]
9. Berg, S. The advantages and disadvantages of the inclusion of students with disabilities into regular education classrooms. In Proceedings of the 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering, Vilnius, Lithuania, 8–10 November 2018; p. 50.
10. Jnoub, N.; Klas, W. Detection of Tampered Images Using Blockchain Technology. In Proceedings of the ICBC 2019—IEEE International Conference on Blockchain and Cryptocurrency, Seoul, Korea, 14–17 May 2019; pp. 70–73. [CrossRef]
11. Weber, I.; Lu, Q.; Tran, A.B.; Deshmukh, A.; Gorski, M.; Strazds, M. A Platform Architecture for Multi-Tenant Blockchain-Based Systems. In Proceedings of the 2019 IEEE International Conference on Software Architecture (ICSA), Hamburg, Germany, 25–29 March 2019; pp. 101–110. [CrossRef]
12. Zhang, M.; Wang, S.; Zhang, P.; He, L.; Li, X.; Zhou, S. Protecting Data Privacy for Permissioned Blockchains Using Identity-Based Encryption. In Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 15–17 March 2019; pp. 602–605. [CrossRef]
13. Zhaofeng, M.; Xiaochang, W.; Jain, D.K.; Khan, H.; Hongmin, G.; Zhen, W. A Blockchain-Based Trusted Data Management Scheme in Edge Computing. *IEEE Trans. Ind. Inform.* **2020**, *16*, 2013–2021. [CrossRef]
14. Ramkumar, M. A Blockchain Based Framework for Information System Integrity. *China Commun.* **2019**, *16*, 1–17. [CrossRef]
15. Martens, D.; Maalej, W. ReviewChain: Untampered Product Reviews on the Blockchain. In Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, New York, NY, USA, 27 May 2018; pp. 40–43. [CrossRef]
16. Salman, T.; Zolanvari, M.; Erbad, A.; Jain, R.; Samaka, M. Security Services Using Blockchains: A State-of-the-Art Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 858–880. [CrossRef]
17. Yang, W.; Aghasian, E.; Garg, S.; Herbert, D.; Disiuta, L.; Kang, B. A Survey on Blockchain-Based Internet Service Architecture: Requirements, Challenges, Trends, and Future. *IEEE Access* **2019**, *7*, 75845–75872. [CrossRef]
18. Takaoğlu, M.; Özer, Ç.; Parlak, E. Blokzinciri Teknolojisi ve Türkiye'deki Muhtemel Uygulanma Alanları. *Int. J. East Anatol. Sci. Eng. Des. (IJEASED)* **2019**, *1*, 260–295. Available online: https://dergipark.org.tr/tr/pub/ijeased/issue/47170/643683 (accessed on 21 September 2021).
19. Pradeepkumar, D.S.; Singi, K.; Kaulgud, V.; Podder, S. Evaluating Complexity and Digitizability of Regulations and Contracts for a Blockchain Application Design. In Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, Gothenburg, Sweden, 27 May–3 June 2018; pp. 25–29. [CrossRef]
20. Tabares-Soto, R.; Arteaga-Arteaga, H.B.; Mora-Rubio, A.; Bravo-Ortíz, M.A.; Arias-Garzón, D.; Grisales, J.A.A.; Jacome, A.B.; Orozco-Arias, S.; Isaza, G.; Pollan, R.R. Strategy to Improve the Accuracy of Convolutional Neural Network Architectures Applied to Digital Image Steganalysis in the Spatial Domain. *PeerJ Comput. Sci.* **2021**, *7*, 1–21. [CrossRef]
21. Xie, G.; Ren, J.; Marshall, S.; Zhao, H.; Li, H. A New Cost Function for Spatial Image Steganography Based on 2D-SSA and WMF. *IEEE Access* **2021**, *9*, 30604–30614. [CrossRef]

22. Sarkar, P.; Ghosal, S.K.; Sarkar, M. Stego-Chain: A Framework to Mine Encoded Stego-Block in a Decentralized Network. *J. King Saud Univ. Comput. Inf. Sci.* **2020**, *16*, 25–29. [CrossRef]
23. Mohsin, A.H.; Zaidan, A.A.; Zaidan, B.B.; Mohammed, K.I.; Albahri, O.S.; Albahri, A.S.; Alsalem, M.A. PSO–Blockchain-Based Image Steganography: Towards a New Method to Secure Updating and Sharing COVID-19 Data in Decentralised Hospitals Intelligence Architecture. *Multimed. Tools Appl.* **2021**, *80*, 14137–14161. [CrossRef] [PubMed]
24. Basuki, A.I.; Rosiyadi, D. Joint Transaction-Image Steganography for High Capacity Covert Communication. In Proceedings of the 2019 International Conference on Computer, Control, Informatics and its Applications (IC3INA), Tangerang, Indonesia, 23–24 October 2019; pp. 41–46. [CrossRef]
25. Partala, J. Provably Secure Covert Communication on Blockchain. *Cryptography* **2018**, *2*, 18. [CrossRef]
26. Horng, J.H.; Chang, C.C.; Li, G.L.; Lee, W.K.; Hwang, S.O. Blockchain-Based Reversible Data Hiding for Securing Medical Images. *J. Healthc. Eng.* **2021**, *2021*. [CrossRef] [PubMed]
27. Xu, M.; Wu, H.; Geng, G.; Zhang, X.; Ding, F. Broadcasting steganography in the blockchain. In *International Workshop on Digital Watermarking*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 256–267.
28. Matzutt, R.; Hiller, J.; Henze, M.; Ziegeldorf, J.H.; Müllmann, D.; Hohlfeld, O.; Wehrle, K. A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin. In *Financial Cryptography and Data Security*; Meiklejohn, S., Sako, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2018; pp. 420–438.
29. Giron, A.A.; Martina, J.E.; Custódio, R. Steganographic Analysis of Blockchains. *Sensors* **2021**, *21*, 4078. [CrossRef]
30. Hassaballah, M.; Hameed, M.A.; Awad, A.I.; Muhammad, K. A Novel Image Steganography Method for Industrial Internet of Things Security. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7743–7751. [CrossRef]
31. Onuma, K.; Miyata, S. A Proposal for Correlation-Based Steganography Using Shamir's Secret Sharing Scheme and DCT Domain. In Proceedings of the 2021 International Conference on Information Networking (ICOIN), Jeju Island, Korea, 13–16 January 2021; pp. 255–260. [CrossRef]
32. Sengupta, A.; Rathor, M. Crypto-Based Dual-Phase Hardware Steganography for Securing IP Cores. *IEEE Lett. Comput. Soc.* **2019**, *2*, 32–35. [CrossRef]
33. Ghosal, S.K.; Mukhopadhyay, S.; Hossain, S.; Sarkar, R. Exploiting Laguerre Transform in Image Steganography. *Comput. Electr. Eng.* **2021**, *89*, 106964. [CrossRef]
34. Wahab, O.F.A.; Khalaf, A.A.M.; Hussein, A.I.; Hamed, H.F.A. Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques. *IEEE Access* **2021**, *9*, 31805–31815. [CrossRef]
35. Kasapbasi, M.C. A New Chaotic Image Steganography Technique Based on Huffman Compression of Turkish Texts and Fractal Encryption with Post-Quantum Security. *IEEE Access* **2019**, *7*, 148495–148510. [CrossRef]
36. Saad, A.H.S.; Mohamed, M.S.; Hafez, E.H. Coverless Image Steganography Based on Optical Mark Recognition and Machine Learning. *IEEE Access* **2021**, *9*, 16522–16531. [CrossRef]
37. Sharifzadeh, M.; Aloraini, M.; Schonfeld, D. Adaptive Batch Size Image Merging Steganography and Quantized Gaussian Image Steganography. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 867–879. [CrossRef]
38. Kordov, K.; Zhelezov, S. Steganography in Color Images with Random Order of Pixel Selection and Encrypted Text Message Embedding. *PeerJ Comput. Sci.* **2021**, *7*, 1–21. [CrossRef]
39. Rodriguez-Garcia, M.; Sicilia, M.A.; Dodero, J.M. A Privacy-Preserving Design for Sharing Demand-Driven Patient Datasets over Permissioned Blockchains and P2P Secure Transfer. *PeerJ Comput. Sci.* **2021**, *7*, 1–25. [CrossRef]
40. Lian, W.; Li, Z.; Guo, C.; Wei, Z.; Peng, X. FRChain: A Blockchain-Based Flow-Rules-Oriented Data Forwarding Security Scheme in SDN. *KSII Trans. Internet Inf. Syst.* **2021**, *15*, 264–284. [CrossRef]
41. Ali, A.; Ahmed, M.; Khan, A.; Anjum, A.; Ilyas, M.; Helfert, M. VisTAS: Blockchain-Based Visible and Trusted Remote Authentication System. *PeerJ Comput. Sci.* **2021**, *7*, 1–26. [CrossRef]
42. Akhtar, M.M.; Khan, M.Z.; Ahad, M.A.; Noorwali, A.; Rizvi, D.R.; Chakraborty, C. Distributed Ledger Technology Based Robust Access Control and Real-Time Synchronization for Consumer Electronics. *PeerJ Comput. Sci.* **2021**, *7*, 1–16. [CrossRef]
43. Shrestha, A.K.; Vassileva, J.; Joshi, S.; Just, J. Augmenting the Technology Acceptance Model with Trust Model for the Initial Adoption of a Blockchain-Based System. *PeerJ Comput. Sci.* **2021**, *7*, 1–38. [CrossRef]
44. Yu, B.; Li, X.; Zhao, H. PoW-BC: A PoW Consensus Protocol Based on Block Compression. *KSII Trans. Internet Inf. Syst.* **2021**, *15*, 1389–1408. [CrossRef]
45. Pranto, T.H.; Noman, A.A.; Mahmud, A.; Haque, A.B. Blockchain and Smart Contract for IoT Enabled Smart Agriculture. *PeerJ Comput. Sci.* **2021**, *7*, 1–29. [CrossRef] [PubMed]
46. International Business Machines Corporation. Why New Off-Chain Storage Is Required for Blockchains. Available online: https://www.ibm.com/downloads/cas/RXOVXAPM#:~{}:text=Because%20non-transaction%20data%2C%20such,off-chain%20data%20is%20unstructured (accessed on 23 September 2021).
47. Nguyen, B.M.; Dao, T.C.; Do, B.L. Towards a Blockchain-Based Certificate Authentication System in Vietnam. *PeerJ Comput. Sci.* **2020**, *2020*. [CrossRef] [PubMed]
48. Xu, X.; Pautasso, C.; Zhu, L.; Lu, Q.; Weber, I. A pattern collection for blockchain-based applications. In Proceedings of the ACM International Conference Proceeding Series, Irsee, Germany, 4–8 July 2018. [CrossRef]