International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Digital Image Steganography in the Spatial Domain Using Block-Chain Technology to Provide Double-Layered Protection to Confidential Data Without Transferring the Stego-Object

[1]K.S. Suresh*, [2]Dr.T. Kamalakannan

Submitted: 20/10/2022 **Revised:** 23/12/2022 **Accepted**: 21/01/2023

Abstract*:* The block-chain technology is an emerging trend in the distributed ledger model, and it gives a security feature to all the nodes and their data. Steganography is also helping the user with private data transmission. These two technologies tightly tie up together to make a new model in the data security field. All the conventional steganography algorithms should transfer the stego-object from one end to another. During the transmission time, if an intruder attacks the stego-object, the receiver cannot retrieve the sender's original messages. The proposed method overcomes this issue, using block-chain technology with the hashing technique and linked list data structures. Instead of transmission of stego-object, only the linked list and the stego-key values only transmitted in the block-chain technology from one end to another. Every data in the linked list and stego-object are secured with CRC. The block-chain technology also provides the second layer of protection to the confidential data with the hash values. Suppose any node in block-chain got modified by an intruder. In that case, the network itself is identified using the hash index value, and the intruder cannot be able to get access to the messages and cannot attack all the nodes in the block-chain network. In general, all the steganography algorithms create a stego-object then we have to compare that with the existing models' output with the two different parameters like payload and distraction of the stego-object. But the proposed method does not create the stego-object; instead of the stego-object, it creates a list of values and passes through the block-chain technology, so output values are not compared with the existing models.

Keywords*: block-chain, steganography, intruder, stego-object, CRC, hash value.*

1. Introduction

Recently, humans have been entirely dependent on the internet solemnly. This era shares the secret message in different forms from one end to another quickly. Most of the secret messages sharing applications are failed to secure the messages [1]. Initially, the crypto algorithms are used to secure secret messages; in later days, these algorithms are easily brute-forced by intruders. The application developers were seeking new technology to secure their messages, and then they found an old idea called steganography [2]; this name came from ancient Greek history, which covered writing. The secret information is shared in war fields, such as written on a cleanly shaved soldier's head, in extinct animal bodies, microdots between letters, and using invisible ink in a neat cloth [3]. This ideology is converted into a digital medium called digital steganography, in which the covered mediums are text files, audio files, video files, and image files [4]. The user can choose their covered medium and design their new algorithms based on their needs. Most of the users are shown their interest in digital image steganography to develop their ideas. All the steganography algorithms produce the stego-objects, and all the stego-objects are shared in a network medium to reach the other end [5]. During the transmission time, if any intruder damages the stego-object, the receiver has no idea about that, and the stego-object fails to produce the secret message properly. To overcome this issue, the proposed image steganography in a spatial domain method suggests that the user need not share the stego-image with another end. Instead, the hash table is shared from one end to the other. The hash table is designed to maintain the self-security of the data with the help of hashing algorithms. If the hash table comes across any attack, the receiver can quickly identify that and send the flagged acknowledgement to the sender. The proposed method is a new era of digital image steganography in the spatial domain and blasts the common barrier of the existing steganography algorithms [6]. When the steganography algorithms use a carrier file as an image file and produce the output as a stego-image, the stego-image file is compared with existing algorithms values with the two parameters, payload size and stego-image quality. This

[1]*Dept. of Computer Science, Rajeswari Vedachalam Government Arts College, Chengalpattu, Research Scholar, VISTAS, Chennai, India. Email. ksampathsuresh@gmail.com*

[2]*Head, Department of Information Technology, School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India. Email: kkannan.scs@velsuniv.ac.in*
**Corresponding Author Email: ksampathsuresh@gmail.com*

model is not preparing a stego-image while the carrier file is an image file; instead on that, it gives only a hash list, then we don't have any parameters to compare with existing models, and the user has no limitations for the payload; they can embed the bits as much as they need. The hash table made itself to identify if any attack happens; it gives healthy security to the private data.

1.1. Block-Chain Technology

The growth of block-chain technology in India augmented nearly 102.54 % it may expect to rise more in the future. Block-chain technology is analogous to the internet. This technology is widely used in cryptocurrencies, but bitcoins and block-chain technology are not identical [7]. Bitcoin is one of the best applications which is used block-chain Straight forward in this network. The block-chain's pointers and linked list data structures are commonly used to store user data and create a chain between the two nodes. A node contains a hash value to secure the data and pointer value of the next node in the network. Every ten seconds, the minor verifies every node in the network; the same has to be done before a single element is added to the network. It has an authorization and verification-enabled model to share all the data in various networks [10]. It has a time-stamping procedure and data loss production. Every transaction in this network is easily traceable.

Merging this block-chain technology with steganography provides good security to the user data on both ends; it has a hashing technology to secure the data while transmitting from one end to another. Steganography is the modern era's digital data-hiding model, and block-chain technology is a current distributed network model to make a note of data movement [11]. The proposed method combines these two technologies to share the secret data from unauthorized users.

2. Background Studies

The data-hiding steganography method has four major divisions: image, audio, video, and text. The primary research papers fall on image-based steganography methods [3]. The image-based models are also classified into two different models, namely the spatial domain and the transform domain, in that the proposed model comes under the spatial domain. In the spatial domain, the confidential data bits were embedded into the carrier image pixel with minimal destructions in a different pattern [12]. In a transform domain, the source image size is minimized and inserted in another image. While comparing these two methods, the spatial domain is more straightforward to implement because most of the research activities happen in the image steganography model in the spatial domain [6]. The spatial domain has a multi-level of branches; in that the main branches are known as the least significant bit data insertion, based on the pixel value differencing technology. It uses the distributed ledger architecture. Block-chain is classified into three different models public, private and consortium [8]. In a public block-chain architecture, data and access permission can be done by all the users in the network. The private block-chain technology is organization-based; the specific user has permission to access data.

The consortium network is a combination of a few organizations that own the network; in this, data is controlled by allocated users. A single user in block-chain technology, denoted by a node, consists of a copy of every network transaction [9]. The distributed data transmission model is used in this technology; every node has all the transaction details. If any node crashes, data recovery is

data bits were inserted, edge-based data insertion, multi-base notational systems are used to insert the data into the image and matrix-based data insertion.

In all the spatial methods, the secret data bits were embedded into the carrier image and produced a stego-image [3][1]. The steganography model commonly passes the stego-object from one end to another; the stego-object consists of secret data bits. If it faces any attack during transmission, then the stego-object fails to produce the proper output; this is said to be a total failure of the secret communication. The receiver should be aware of that; whether the stego-object has been brute-forced [13].

2.1. LSB Models: Embedding the least significant bit (LSB) Each pixel in a grayscale image has an 8-bit representation. Since the value of the last bit in a pixel will only change the value by one, it is known as the Least Significant Bit [14]. Therefore, the data in the source file is hidden using this property. In this case, the last two bits have been treated as LSB bits because they will only change the pixel value by "3". This helps in storing additional information. Encrypt the raw data before embedding it in the image to increase security because this method is susceptible to steganalysis [15]. Although the encryption process adds to the complexity and length of the procedure, it also offers increased security. [6] This approach substitutes a bit of the secret message for the least significant bits of any or every pixel inside a carrier image. Numerous methods for concealing messages within multimedia carrier data have evolved from the LSB embedding approach [16]. LSB embedding can be used with a wide range of data types and formats. As a result, LSB embedding is the prominent one among the most significant steganographic techniques that are in use now [17].

Data is randomly hidden in this technique, i.e., it is hidden in a randomly chosen pixel. The Fibonacci algorithm is used to produce random pixels [18]. The occurrence of identifiable artefacts in the form of pairs of values is the

fatal flaw of LSB embedding (PoVs). The suggested approach alters the typical distribution of (PoVs) in the histogram domain, making steganalysis more challenging and consequently boosting security [19]. This consistent equality pattern, often known as the PoVs artefact, is rare for the histogram domain. The user-specified stego-key generates a set of predetermined thresholds that determine whether to increment or decrement the sample value [20]. The model [21] takes advantage of every edge pixel in a picture. Here, we mask the two LSB bits in the cover picture to calculate the masked image first. Then, we use the Canny Edge detection technique to locate the edge pixels [22]. Once we've got the edge pixels, we only transmit the stego image to the recipient after hiding the data in the edge pixels' LSB bits. Different kinds of cover media are used in steganography techniques for the embedding process [12].

Every digital format is a cover medium for secret messages hidden inside audio, video, text, digital images, or even network protocols like TCP. This technique is known as protocol steganography [23].

2.2. PVD Models: A perfect square-based PVD scheme has been put out by [24] PVD, and the LSB substitution was combined with increasing both capacity and undetectability. They used the PVD technique if the difference in pixel values was greater than 15, else they used the 3-bit LSB substitution. Used modified LSB substitution after classifying the 3x3 pixel blocks into four models, and compared to [25] methodology, this method has a better embedding capacity and less distortion. [26] discovered that histogram-based analysis may be used to identify the PVD process. Step effects can be seen in the pixel variance histogram. [24] A PVD technique known as the side match method is based on the choice to embed data on a target pixel on the values of pixels nearby. [27] The technique had a fall-in-error issue. Furthermore, side match approaches based on the greatest difference between nearby pixel values have been suggested to increase hiding capability. According to [20][28], histogram-based attacks can identify this strategy. So, [29] they suggested a modulus function-based improvement to PVD.

2.3. Blockchain Technology Models: A method based on the same model and utilizing modification directions was proposed by [30]. It [7] ensures the authenticity and irrefutability of digital content. The authors' solution addresses the issue that the user's secret key does not contain the user's specific information when it is shared with other entities. Analysing the secret key's origin becomes challenging if the public key is compromised or misused. A bottleneck for current systems is the loss of private data in access control [31]. As a result, authors have included the attribute-based encryption privacy protection mechanism to safeguard private keys [32]. Decryption mechanisms, however, do not demonstrate increased efficacy. To ensure digital data protection, information rights management is a crucial prerequisite. Transparency, decentralization, and trust are lacking in currently used data rights strategies. The model discussed in [10] gives a decentralized blockchain-based solution. Everyone has access to information on the usage of digital content, including transaction and licence details. Smart contracts are made to assign licences automatically [23]. Through this approach, the owner may establish the price at which the licence is sold to other customers.

However, in order to accomplish the critical acquisition, network peers must have powerful computers. The authors [10] list out a blockchain-based digital rights management to stop the illegal use of private digital content. For these issues, a solution known as DRM chain is suggested. This system guarantees that authenticated users will use digital content appropriately. [33] paper to identify the incentive processes using the pre- and post-results following empirical study, a review of health-related and medical data was undertaken. Per the survey, a single incentive is evaluated for medical and health-related data to determine the rate of data sharing [34].

3. Proposed Method

The proposed method initially begins with the data conversion of the secret message into binary bits step by step. These bits are divided into binary blocks as follows; every consecutive eight bits are grouped as one block. Each block of binary bits is changed into a decimal equivalent and stored in a list from the sender side. It is depicted in figure 1 as follows.

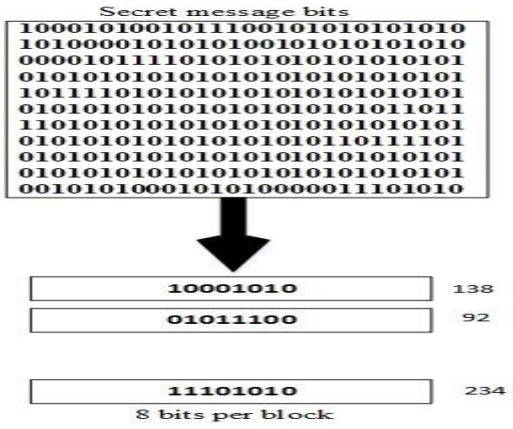

Fig. 1. Secret Message conversion

In this proposed method, users have some restrictions on preparing the image list on their sides. Both sides have an identical group of images, which should be stored in the list in sequential order. The carrier image should have all values between 0 to 255 at minimum once in the image, which satisfies the above-said condition; these images are only stored in the list. On both sides, the image list has only eight images; these images are denoted in a binary number from 000 to 111, and that notation is used in the

stego-key preparation on the sender side. The user has four different scanning options to scan the selected image. The scan types are depicted as follows in figure 2. The scanning models are (a) Column wise scanning, (b) Row wise scanning, (c)In-Spiral, and (d) Out-Spiral. The user selects the scan type; the carrier image has been scanned and develops a location array.

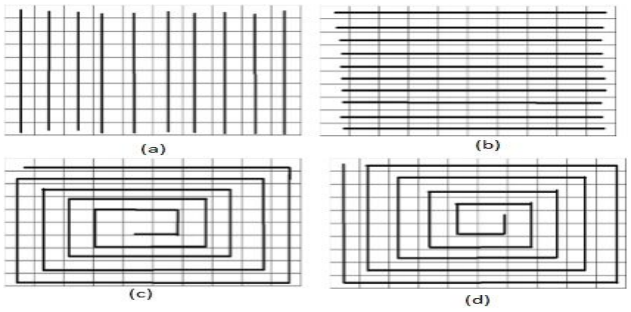

Fig. 2. Scan types

The location array contains 17 rows and 15 columns which are used to accommodate 255 values only. The first occurrence of every pixel value from one to 255 in the carrier image has to be stored in the array in sequential order. The pixel value zero is maintained separately in the variable; for example, pixel value 18 is stored in a second-row third value (2,3), and 25 is fixed in the second-row tenth position (2,10). The same is shown in the following Table 1.

Row / Col	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
3	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
4	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
5	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
6	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
7	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105
8	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
9	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135
10	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150
11	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165
12	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180
13	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195
14	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210
15	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225
16	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240
17	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

Table 1. Location Array

The location array is used to identify whether all the values are present in the carrier image or not. If any value between 1 – 255 is missing, then the carrier image is considered invalid, and the hiding process is stopped. Then the hash table is built based on the location array; it should contain all the pixel values. A hash table consists of two columns: pixel value and array index of the same pixel value in the location array. The proposed method uses hashing technique and it attains the best case of space and time complexity. Table 2. shows the sample hash table.

Pixel value	Array index
1	12,05
2	13,2
3	2,6
4	7,3
5	13,8
6	16,9
7	5,12
8	4,8
9	11,2
10	12,3
.	.
.	.
.	.
.	.
.	.
253	17,3
254	14,9
255	11,6

Table 2. Hash Table

Once the pixel value hash table is created, the sender side deletes the location array. The next level of security upliftment is done in the hash table by adding the CRC value. The CRC polynomial table has four different choices, and each of them is denoted by binary notation from 000 to 011. The equivalent polynomial value is generated based on the choice of using the CRC polynomial, as shown in Table 3.

CRC index value	CRC Polynomials	CRC Polynomial value
000	$X^3 + X + 1$	1011
001	$X^3 + X^2 + 1$	1101
010	$X^3 + X^2 + X + 1$	1111
011	$X^3 + 1$	1001

Table 3. CRC Polynomial Table

The CRC hash table is generated with the help of a polynomial value, which is obtained from the polynomial table. CRC hash table values are calculated as follows; every array index column value from the CRC table is modulo division by the polynomial value of the CRC then the remainder is stored in the same position of the hash table; after all the elements are done, the table is called as CRC hash table, it is shown in the CRC Hash table (Table 4.).

Array index	CRC Checker
1	100
2	101
3	110
4	001
5	010
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
.	.
252	110
253	100
254	101
255	001

Table 4. CRC Hash Table

Once all the above-said processes are done, Table 5. Shows the stego-key is prepared to follow the given structure; this structure has 12 bits sequentially. Every three bits were allotted for storing the image, scan, and CRC index values. The last column value added by these nine bits is modulo divided by the CRC value selected by the user. The remainder value is accommodated in the last three positions in the stego-key by way of this last step strengthens the stego-key's security on the sender side. Table 6. shows the sample stego- key.

Stego-Key	Image Index Value	Scan Index Value	CRC Index Value	CRC Bits
	3 bits	3 bits	3 bits	3 bits

Table 5. Structure of Stego-key

Stego-Key	Image Index Value	Scan Index Value	CRC Index Value	CRC Bits
	111	011	001	010

Table 6. Sample Stego-key

The message passing linked list creating procedure is as follows; initially, the secret messages are converted into n blocks, and each block converts into decimal numbers. Each decimal number identifies the position in the CRC hash value table; that value and the CRC checker are stored in the data part of the message passing linked list, and the linked part is used to connect to the next value. If the decimal value already exists in the linked list, the procedure does not create a new location to store the value again. It establishes the link for the current value. Using this idea, the embedding procedure can embed more secret message bits without any restrictions.

Finally, the message passing the linked list has the full nodes that should exceed the limits of 255 nodes. Below, figure 3 shows the embedding procedure of the proposed method on the sender side. The message passing linked list and stego-key are created on the sender side. The linked list and the stego-key transfer from one end to another using block-chain technology. The sender and receiver create a node in the private block-chain technology. This technology is well-known for sharing personal data, but sharing images using this technology is not easy. The main advantage of block-chain technology is that all the information is stored in every network node. Every message is encrypted by hashing algorithms. If any intruder gets the single node information, the hash value is automatically changed, and the connection to the next node is broken down; with these security features, the message is passed from one end to another in safe mode. The proposed method uses this block-chain technology to transfer the stego-key and the message passing the linked list.

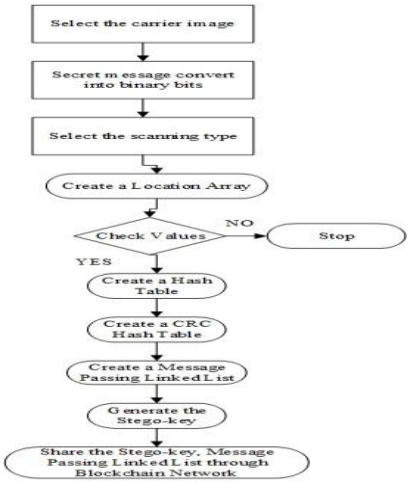

Fig. 3. sender-side data embedding flow chart

4. Developing Hyperledger Fabric in a block-chain platform

Hyperledger Fabric is a block-chain platform for distributed ledger solutions underpinned by a modular architecture delivering high degrees of confidentiality, resiliency, flexibility, and scalability. It is designed to support pluggable implementations of different components: Ledger, Membership Service Provider, Smart Contract, Peers, Ordering Service, Channel, Certificate Authority, and Organizations. The above components are created using the solidity programming language. In this architecture, ordering services are applied of to send and receive a message by the users. The block-chain has a secured transmission with the certificate authority; the proposed method also uses a hash model, which helps to protect the user data well.

If any intruder attacks the technology, they may get only a single bit of information, not whole data; if anything happens, this network is automatically identified by miners. Miners check all the nodes in frequent intervals. The following figure depicts the architecture of this block-chain technology.

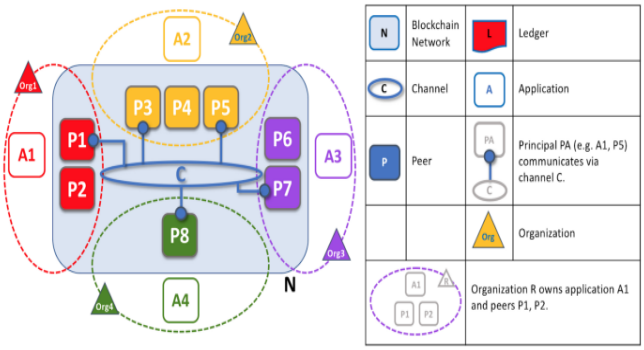

Fig. 4. Block-Chain model

Once the above model (Figure 4.) is created, the message passes from one end to another. Once the data has been received at another side, the data retrieval process starts. On the receiver side, once the stego-key is received, the reverse engineering process starts to recover the message bit from the linked list. The stego-key plays a vital role in getting back the information; initially, check whether any intruder cracks the stego-key or not; this process is done by CRC value. The first nine bits are modulo divided by the CRC index value. If it produces the CRC bits correctly, the receiver can quickly identify that the stego-key is not brute-forced; otherwise, the receiver sends the wrong acknowledgement message to the sender to send the same message again. The stego-key has 12-bit serial binary bits; used to identify which image is used on the sender side, which scan type is utilized by the sender, then select the carrier image and scan the image with the scan type creates the location array. Suppose all the values are in the Array move to the next step creating a hash table with the help of CRC polynomial value. Increasing the self-protection layer creates a CRC hash table. In that table, every value should equal what passes through the block-chain technology. If all the process gives a sound output, then binary bits are converted into ASCII and arranged in sequential order. Then only the receiver side gets the original message correctly.

5. Result and Discussion

The conventional steganography models transmit the stego-object from one to another, but this proposed method is not transferring the carrier image; instead of that, it passes only the hash table in the block-chain technology with double-layered security with a high level of payload. The traditional model has some payload restrictions, but this model doesn't have a payload restriction; the user can share any amount of data from one end to another. The data is not accommodated in the carrier image that will be stored in a table with CRC protection. The proposed method creates a linked list only because it will not compare with the conventional steganography models.

6. Conclusion

Initially, cryptography algorithms are used to protect the user data from an unauthorized person, but it has been compromised after some point. At this particular time, the steganography models are provoking the same process. In the conventional models, the carrier file got an attack during the transmission time; the receiver side has no idea about that. Due to that, it may fail to produce the correct results. The proposed model has some unique features; with this help, the user can share more data bits without restriction; if an intruder attacks the hash table, the receiver can quickly identify that. The above model protects the user data in double-layered protection as follows CRC and hashing values in the block-chain technology. The proposed model shakes hands with block-chain technology to protect the end-user data in double-layered security and without any payload restriction with zero damage to a carrier image file. The future scope of this paper is the user can develop a new model to incorporate current technologies like ML, Deep Learning and AI.

References

[1] C. Navadiya and N. Sanghani, “Comparative Survey of Digital Image Steganography Spatial Domain Techniques,” in *Lecture Notes on Data Engineering and Communications Technologies*, vol. 52, 2021.

[2] B. Siddiqui and S. Goswami, “a Survey on Image Steganography Using Lsb Substitution Technique,” *Int. Res. J. Eng. Technol.*, 2017.

[3] P. Agrawal and A. Upadhyay, “A Survey of Different Steganography Technique using Cryptographic Algorithm,” *Asian J. Comput. Sci. Technol.*, vol. 7, no. 2, 2018, doi: 10.51983/ajcst-2018.7.2.1884.

[4] J. Li, X. Wang, Z. Huang, L. Wang, and Y. Xiang, “Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing,” *J. Parallel Distrib. Comput.*, vol. 130, 2019, doi: 10.1016/j.jpdc.2019.04.003.

[5] A. G. Salman, Rojali, and Vivi, “Steganography using pixel value differencing spiral,” *J. Theor. Appl. Inf. Technol.*, vol. 75, no. 1, 2015.

[6] O. C. Abikoye and R. O. Ogundokun, “Efficiency of LSB steganography on medical information,” *Int. J. Electr. Comput. Eng.*, vol. 11, no. 5, 2021, doi: 10.11591/ijece.v11i5.pp4157-4164.

[7] M. Naz *et al.*, “A Secure Data Sharing Platform Using Blockchain and Interplanetary File System,” *Sustain.*, vol. 11, no. 24, pp. 1–24, 2019, doi: 10.3390/su11247054.

[8] J. Sun, X. Yao, S. Wang, and Y. Wu, “Blockchain-Based Secure Storage and Access Scheme for

Electronic Medical Records in IPFS," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS. 2020.2982964.

[9] J. Guo, C. Li, G. Zhang, Y. Sun, and R. Bie, "Blockchain-enabled digital rights management for multimedia resources of online education," *Multimed. Tools Appl.*, vol. 79, no. 15–16, 2020, doi: 10.1007/s11042-019-08059-1.

[10] Z. Zhang and L. Zhao, "A design of digital rights management mechanism based on blockchain technology," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018, vol. 10974 LNCS, doi: 10.1007/978-3-319-94478-4_3.

[11] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, 2018, doi: 10.1016/j.cose.2018.06.004.

[12] G. L. Smitha and E. Baburaj, "A survey on image steganography based on block-based edge adaptive based on Least Significant Bit Matched Revisited (LSBMR) algorithm," 2017, doi: 10.1109/ICCICCT.2016.7987931.

[13] D. N. Aini, D. R. I. M. Setiadi, S. N. Putro, E. H. Rachmawanto, and C. A. Sari, "Survey of Methods in the Spatial Domain Image Steganography based Imperceptibility and Payload Capacity," 2019, doi: 10.1109/ISEMANTIC.2019.8884333.

[14] G. Swain, "Digital image steganography using nine-pixel differencing and modified LSB substitution," *Indian J. Sci. Technol.*, vol. 7, no. 9, 2014, doi: 10.17485/ijst/2014/v7i9.27.

[15] K. Bansal, A. Agrawal, and N. Bansal, "A Survey on Steganography using Least Significant bit (LSB) Embedding Approach," 2020, doi: 10.1109/ICOEI48184.2020.9142896.

[16] H. Zhou, W. Zhang, K. Chen, W. Li, and N. Yu, "Three-Dimensional Mesh Steganography and Steganalysis: A Review," *IEEE Trans. Vis. Comput. Graph.*, 2021, doi: 10.1109/TVCG.2021.3075136.

[17] M. Pavani, S. Naganjaneyulu, and C. Nagaraju, "A Survey on LSB Based Steganography Methods," 2013.

[18] S. S. N. Bhuiyan, N. A. Malek, O. O. Khalifa, and F. D. A. Rahman, "An improved image steganography algorithm based on PVD," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 10, no. 2, 2018, doi: 10.11591/ijeecs.v10.i2.pp569-577.

[19] S. SOLAK and U. ALTINIand350IK, "LSB Substitution and PVD performance analysis for image steganography," *Int. J. Comput. Sci. Eng.*, vol. 6, no. 10, 2018, doi: 10.26438/ijcse/v6i10.14.

[20] J. Chen, "A PVD-based data hiding method with histogram preserving using pixel pair matching," *Signal Process. Image Commun.*, vol. 29, no. 3, 2014, doi: 10.1016/j.image.2014.01.003.

[21] A. O. Modupe, A. E. Adedoyin, and A. O. Titilayo, "A Comparative Analysis of LSB, MSB and PVD Based Image Steganography," *Int. J. Res. Rev.*, vol. 8, no. 9, 2021, doi: 10.52403/ijrr.20210948.

[22] N. J. R. Rao, "Data Hiding using Edge-based Image Steganography," *Int. J. Sci. Res.*, vol. 6, no. 4, pp. 176–180, 2017, [Online]. Available: https://www.ijsr.net/archive/v6i4/ ART20172193.pdf.

[23] R. K. S. Et. al., "Digital Transformation In Indian Insurance Industry," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 4, 2021, doi: 10.17762/turcomat.v12i4.509.

[24] C. C. Chang and H. W. Tseng, "A steganographic method for digital images using side match," *Pattern Recognit. Lett.*, vol. 25, no. 12, 2004, doi: 10.1016/j.patrec.2004.05.006.

[25] S. A. Thanekar and S. S. Pawar, "OCTA (STAR) PVD: A different approach of image steganopgraphy," 2013, doi: 10.1109/ICCIC.2013.6724139.

[26] G. Swain, "A Steganographic Method Combining LSB Substitution and PVD in a Block," *Procedia Comput. Sci.*, vol. 85, no. Cms, pp. 39–44, 2016, doi: 10.1016/j.procs.2016.05.174.

[27] W. Bin Lin, T. H. Lai, and K. C. Chang, "Statistical feature-based steganalysis for pixel-value differencing steganography," *EURASIP J. Adv. Signal Process.*, vol. 2021, no. 1, 2021, doi: 10.1186/s13634-021-00797-5.

[28] I. H. Pan, K. C. Liu, and C. L. Liu, "Chi-square detection for PVD steganography," 2020, doi: 10.1109/IS3C50286.2020.00015.

[29] J. Salunkhe and S. Sirsikar, "Pixel Value Differencing a Steganographic method: A Survey," *Int. Conf. Recent Trends Eng. Technol. - 2013*, vol. ICRTET 201, 2013.

[30] S. Y. Shen and L. H. Huang, "A data hiding scheme using pixel value differencing and improving exploiting modification directions," *Comput. Secur.*, vol. 48, 2015, doi: 10.1016/j.cose.2014.07.008.

[31] "Exploration of Block Chain Technology in Data Security Field," in *2019 5th International Conference on Advanced Computing, Networking and Security (ADCONS 2019)*, 2019, vol. 1, doi:

10.33969/eecs.v1.007.

[32] S. Muthamilselvan, N. Praveen, S. Suresh, and V. Sanjana, “E-DOC Wallet Using Blockchain,” 2018, doi: 10.1109/CESYS. 2018.8724054.

[33] D. Li, Z. Cai, L. Deng, X. Yao, and H. H. Wang, “Information security model of block chain based on intrusion sensing in the IoT environment,” *Cluster Comput.*, vol. 22, 2019, doi: 10.1007/s10586-018-2516-1.

[34] A. Wu, Y. Zhang, X. Zheng, R. Guo, Q. Zhao, and D. Zheng, “Efficient and privacy-preserving traceable attribute-based encryption in blockchain,” *Ann. des Telecommun. Telecommun.*, vol. 74, no. 7–8, 2019, doi: 10.1007/s12243-018-00699-y.