Intelligent Systems and Computer Technology
D.J. Hemanth et al. (Eds.)

doi:10.3233/APC200113

Blockchain-Based Protected Digital Copyright Management with Digital Watermarking

D.Geethanjali[a,1], Dr.R.Priya[b] Dr.R.Bhavani[b]
[a] Research Scholar, *Dept. of CSE, Annamalai University, India*
[b] Professor, *Dept. of CSE, Annamalai University, India*

Abstract. In the digital era, more and more information is shared through the internet. This may lead to editing, transmitting, misusing detection and usage of information by unauthorized persons. To avoid such a problem we use the digital right management (DRM) with blockchain. In our daily life, blockchain is a powerful utensil to share the data in decentralized and distributed technology. The DRM process provides security and authentication for the content and owner of the data. In our proposed system, the following steps have been implemented Watermark Embedding with Discrete Wavelet Transform (DWT), Arnold Transform (AT), Perceptual Hash, Hash Code generation (md5), Watermark Extraction and Blockchain Creation. Discrete Wavelet Transform provides better image quality and robustness. Arnold Transform provides the best watermark encryption. The hash code generation gives a numeric value which helps in the recognizable proof of a ediget during equality testing. Blockchain is used to store the information in a secured manner and also provide timestamp authentication. Watermark extraction is achieved with the inverse of Arnold transform, inverse Discrete Wavelet Transform with the matching of hash code. This system provides secure transactions with copyright-protected data and safe transparent management.

Keywords. md5 Hash, perceptual hash, Digital right management, blockchain, Arnold Transform, Discrete Wavelet Transform (DWT)

1. Introduction

The rapid evolution of digital technology makes the development of reliable and robust schemes for protecting digital still images, audio, and video from piracy. Piracy attacks include illegal access to transmitted data in networks, data content modification, production and retransmission of illegitimate copies. Innovations of new technology on the internet provides easy transmission of data, reduce the economy and time. But still the security, robustness, content protections are a challenging task in the network media. To solve those problems we can provide copyright authentication with some concealed information [5]. The impact of such attacks might be very large, both in financial and security systems. This paper is organized as follows. Section II gives the Literature review. Section III illustrates the proposed system. Section IV describes the results and discussion. Section V narrates the conclusion and future work of the system.

[1] Geethanjali.D, Research Scholar, Dept. of CSE, Annamalai University, India
Email:anjali.geetha81@gmail.com

1.1 Digital Watermark System

Digital watermarking is the method of hiding a bit of pattern, logo or text inserted into a digital image, audio and video file. It identifies the file's copyright information [13]. Its purpose is to make it more difficult for the original image to be copied or used without permission. It is a process of embedding some information into multimedia digital content [15]. The information can later be extracted or detected for a variety of applications like security and authentication.

1.2 Digital Right Management (DRM)

The digital rights management system is defined, as technological protection in the digital era. It measures a set of access control technologies for restricting the use of proprietary hardware and copyrighted works. It is important to publishers of electronic media since it helps ensure that it will receive the appropriate revenue for their products [4][7]. The purpose of DRM is to prevent unauthorized redistribution of digital media and restrict the ways consumers can copy content they have purchased. It controls the trading, protection, monitoring, modification, distribution, and tracking of digital media, DRM helps publishers limit the illegal propagation of copyrighted works. [11].

1.3 Blockchain

A blockchain is an advanced record of exchanges. The name originates from its structure, wherein singular records, called blocks, are connected together in a solitary rundown, called a chain. Blockchain is a conveyed and decentralized computerized record which records exchanges over a worldwide system of PCs where the data is exceptionally verified [1][2].The various applications areas of blockchain are healthcare, voting, food and supply, real estate, and agriculture.

The blockchain has gained importance due to the following reasons (a) it is decentralized because it is not possessed by a single individual. (b) The data is stored inside cryptographically. (c) It is transparent which means the user's personal information is maintained in a securely way but all the transactions can be viewed as an open-source. (d) It is immutable, so no one can tinker with the data that is inside the blockchain. (e)Accuracy of the chain is attained [8][9]. Blockchain eliminates the need for third-party verification and cost.

The primary block in the blockchain is represented as the genesis block. This has no previous block so the hash value of this block is mentioned as "0000". At the point when another block is added to a blockchain, it is connected to the previous block utilizing a cryptographic hash produced from the substance of the previous block. This guarantees that the chain is rarely broken and that each block is recorded for all time. It is additionally hard to change past transaction in the blockchain since all the ensuing blocks must be modified first.

2 Review of Literature

Harshini V M, et al. [1], the proposed system that handles the authentication of patient data using blockchain. MENG Zhaoxiong, et al. [3] , proposed a combination of digital watermarking and blockchain used to perform the information stored and retrieved from (Interplanetary File System)IPFS in a secured manner with the help of hash code and QR(Quick Response) code. Ma Zhaofeng, et al. [2], proposed a new design Digital Right Management scheme based on watermarking and blockchain to store and provide timestamp authentication of multiple watermarks.

Zhaofeng Ma, et al. [5], proposed productive and secure verification and protection gave by the blockchain interfaces to the enormous size of data. Alexander Savelyev [8], discussed the issues of copyright management system in the network effects. Asaph Azaria, et. al [12], proposed a framework that gives patients a far reaching, unchanging log and simple access to their restorative data across suppliers and treatment destinations. Likewise, they gave Medical record the board, confirmation, secrecy, responsibility and information sharing critical contemplations when taking care of delicate data. Hussain Nyeem, et al. [13], proposed basic watermarking properties and their significance exemplified for various image applications. They additionally characterized a lot of potential assaults utilizing their model demonstrating distinctive winning situations relying upon the abilities. It is visualized that with legitimate thought of watermarking properties and foe activities in various picture applications, the utilization of the proposed model would permit a bound together treatment of all for all intents and purposes.

3. Proposed System

In the current scenario, the available technologies become more transparent and open-source to the public. This creates big challenges of recent years, for managing the data with authentication restrictions and security. The proposed system was implemented in two stages. (i) Watermark process (ii) Blockchain Process. Figure.1 illustrates the proposed system of watermarking and blockchain process.

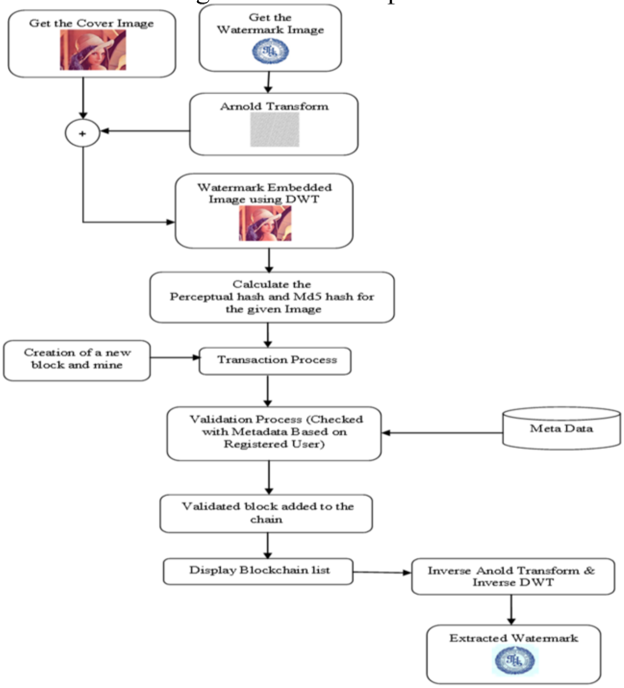

Get the Cover Image
Get the Watermark Image
Arnold Transform
+
Watermark Embedded Image using DWT
Calculate the Perceptual hash and Md5 hash for the given Image
Creation of a new block and mine
Transaction Process
Validation Process (Checked with Metadata Based on Registered User)
Meta Data
Validated block added to the chain
Display Blockchain list
Inverse Anold Transform & Inverse DWT
Extracted Watermark

Figure 1. Block diagram of the Proposed System

In the first stage, (a)/ the cove image is chosen. (b)the number of Arnold Transform (AT) iterations, which increases the encryption strength. (c) The watermark image was embedded on the cover image by using the Discrete Wavelet Transform (DWT) (d) Perceptual hash generates which is a 16-bit hexadecimal value used for the image identification. Cryptographic Hash Code (md5) is generated for the watermarked image. It has a 32-bit value. The two hash values are generated and transferred to the transaction process of the blockchain (e) finally the watermarked image is extracted after the inverse process of Discrete Wavelet Transform and Arnold Transform.

In the second stage, (f) the blockchain was created. Each block has the following block information {index, timestamp, list of transactions, proof, previous block hash}. (g) Adding information to the transaction block. At the time of the transaction process, the md5 hash code was generated which is a 32-bit numeric value and it cannot trace back the original data. (h) The chain for a block, which mentions all the transactions. (i) The validation process confirms whether the block is authorized to block or not by checking with the Metadata. The validated block has to be added to the blockchain ledger. (j) Finally, data instances of the blockchain are displayed.

3.1 Get the Input

The input cover image and watermark image are chosen to perform the embedding and extraction process.

3.2 Arnold Transform (AT)

Two-dimensional Arnold Transform is utilized for the transformation process. The original image is a $N \times N$ two-dimensional array and the coordinate of the pixel is $F = \{(x, y) \mid x, y = 0, 1, 2, . ., N - 1\}$[3]. The encrypted Arnold Transform is represented by

$$\boxed{\begin{pmatrix} xn \\ yn \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x1 \\ y1 \end{pmatrix} \bmod (N) \qquad \text{Eq. (1)}}$$

where xn and yn are the transformed coordinates corresponding to $x1$ and $y1$ after n iterations. The inverse Arnold Transform is represented as follows

$$\boxed{\begin{pmatrix} x1 \\ y1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} xn \\ yn \end{pmatrix} \bmod (N) \qquad \text{Eq. (2)}}$$

Arnold transform is used to encrypt the watermark image to increase security. In handy applications, Arnold Transform not just scrambles the pixel position by encoding the iterative number of the procedure diminishes the key spaces of capacity and transmission.

3.3 Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform is analyzing an image and converting it into a set of mathematical expressions. Later the information can be decoded by the receiver. In the end, watermarking is the solution for this kind of media (images, video) which are in large size. This technique is efficient for image watermarking. The main objective of the Discrete Wavelet Transform technique is to hide data in the form of coefficients

[10]. Embedding in frequency domain watermarking is more robust than the spatial domain.

$$Iw(u,v) = \{I(u,v) + \beta w(x,y), u,v \in HL, LH\ I(u,v), \notin LL, HH\} \quad \text{Eq. (3)}$$

Where, *I(u,v)* and *Iw(u,v)* are the original and watermarked DWT coefficients of the image and *w(x,y)* are the pixels of the watermark. *β* is referred to as a trade-off between robustness and visual perceptibility. Wavelet transform is performed on the image to decompose it into approximation coefficients (LL), horizontal (HL), vertical (LH) and diagonal (HH) detail coefficients of the image.

3.4 Hash Code

Hash code is a numeric value which helps in the recognizable proof of an item during balance testing and furthermore can fill in as a record for the article. The reason for hash code is to help in effective query and inclusion in information assortments which depend on a hash table [14]. The produced numeric value cannot be followed back to the original message information. Hash code has the following advantages like fast computation, collision resistance, widespread use, security and provides a one-way hash. Basically, perceptual hash functions have the following four categories of Hash function namely: Average hash (AHA), Different hash (DHA), Perceptual Hash (PHA), and wavelet hash (WHA). This system generates the perceptual hash which is a 16-bit hexadecimal value. Here Message Digest md5 hash code algorithm is used. It generates 32-bit value [6]. The hash code provides strong security. Second, it provides difficulty to identify or access the original data of the unauthorized persons. The hash values of the sample image are given in figure 2.

imageid = 99c6562d7533a296
imagehash : 2f91ee99129d9dbefe24d28ec9f5f499

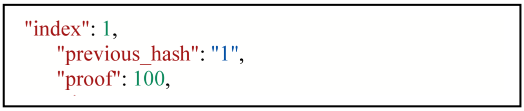
Figure 2. Perceptual Hash code and md5 of image lena.jpg

3.5 Watermark Extraction

The inverse process of Arnold Transform and Discrete Wavelet Transform was applied on the watermarked image. The watermark image was extracted from the cover image at the receiving end.

3.6 Creation of a new block

Blockchain has a blockchain class. It creates and manages the empty list of the chain. The first block of the node is known as a header block or genesis block. It has no predecessors. The new blocks will be mined based on the proof of work (PoW), which covers all the data in the block. The block which is shown below is obtained using the method new_block(). It is used to create a new block which is known as the genesis block. Each new block contains a hash code value.[16] Figure.3 shows the individual block of the data in the blockchain.



```
"index": 1,
    "previous_hash": "1",
    "proof": 100,
```

Figure 3. Individual block of data in the blockchain

3.7 Adding Transactions to the block

The information of hash value and the copyright data of the sample image lena.jpg is added to the transaction block. Here new_transaction() method is used to add a new transaction to the block. The generated new transaction block parameters are given in figure 4.

```
{
    "username": "savesh" ,
    "usermailid": "svrt019@gmail.com",
    "imageid": " 99c6562d7533a296",

"imagehash": " 2f91ee99129d9dbefe24d28ec
9f5f499",
    "title": "lenaimage.png",
```

Figure 4. Adding transactuons to the block

The mine method is used to add a new block to the network. The new node is created in the blockchain network by mining, as shown in figure 5.

```
"index": 2,
"message": "New Block Forged",
"previous_hash": "7855dc14ee66469a02d2d2a3c1cce127",
"proof": 5057,
"transactions": [
{
"amount": 600,
"imagehash": "2f91ee99129d9dbefe24d28ec9f5f499",
"imageid": "99c6562d7533a296",
"recipient": "d259c0ec66e54960a7f5ca5b6bfc9787",
"sender": "6cabd7d85590467b82098ed9af4e6ca5",
"title": "lenaimage.jpg",
"usermailid": "svrt019@gmail.com",
```

Figure 5. Blockchain network coding

3.8 Creation of a blockchain

Each and every block is mined and added to the existing block based on the request by the user. The counts of the total number of blocks are updated accordingly. The chain of the block is built by method, chain. Finally, it returns the whole list of block chains are shown in below:

```
{
 "chain": [
   {
    "index": 1,
    "previous_hash": "1",
    "proof": 100,
    "timestamp": 1576918433.6259363,
    "transactions": []
   },
     {
    "index": 2,
    "previous_hash": "c0f29269181b8ebcd009e7ea013d2c99",
    "proof": 26067,
    "timestamp": 1576918649.5727153,
      "transactions": [
        {
          "amount": 100,
          "imagehash": " 021fb6fd5a9fe39eef22ceb04990d684",
          "imageid": " a392f5f946a439c2",
          "recipient": "5b9cb40adf904360b5e7105d8b9c2fd4",
          "sender": "6cabd7d85590467b82098ed9af4e6ca5",
          "title": "artimage.png",
          "usermailid": "rajan2019@gmail.com",
          "username": "Rajan"
        },
        {
          "amount": 600,
          "imagehash": "2f91ee99129d9dbefe24d28ec9f5f499",
          "imageid": "99c6562d7533a296",
          "recipient": "d3d396c0586d4ef5a98b52470241ecb1",
          "sender": "6cabd7d85590467b82098ed9af4e6ca5",
          "title": "lenaimage.jpg",
          "usermailid": "svrt019@gmail.com",
          "username": "sarvesh"
        }
      ]
    }
  ],
  "length": 2
}
   },
```

3.9 Validation Process of a block

Each node on our network should keep a registry of other nodes on the network. It is performed by using the following method, nodes/register to accept a list of new nodes in the form of URLs (POST method is used). The validation process checks the transaction node whether it is authenticated to the specified network or not. If any divergence occurs, it is determined by using the method, nodes/resolve (GET method is used). It is used to ensure that the node has been added to the correct chain.

3.10 Displaying the blockchain list

The following url http://localhost:5000/chain shows the list of transaction nodes created in the blockchain for our system.

4 Results and Discussion

In our study, we have standard test images of size 512x512. The size of the watermarked image is 128x128. The watermarking process was implemented using MATLAB. The blockchain process was implemented using the Postman API. The sample results are shown below. Figure.6 shows the implemented Watermark Process

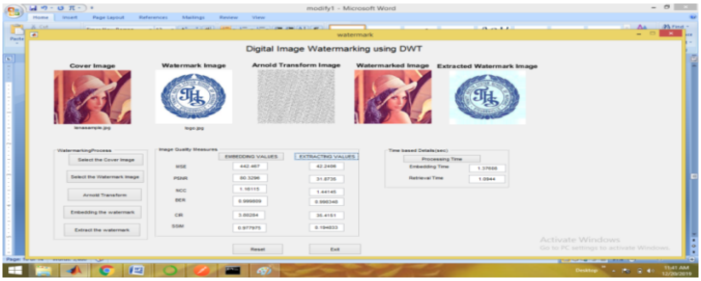


Image Quality Measures

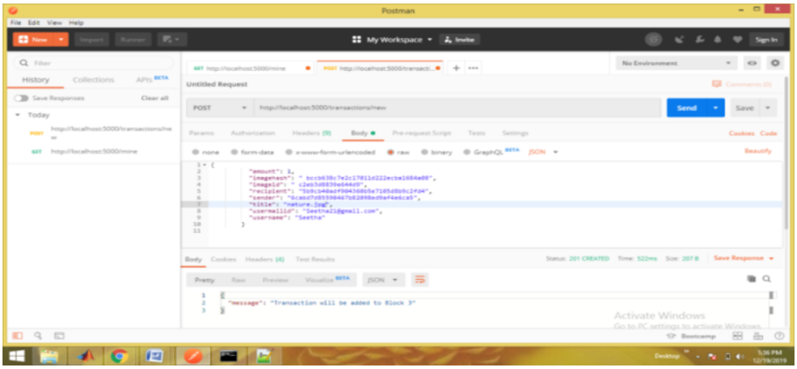
	EMBEDDING VALUES	EXTRACTING VALUES
MSE	442.467	42.2406
PSNR	80.3296	31.8736
NCC	1.16115	1.44145
BER	0.999609	0.998348
CR	3.88284	35.4151
SSIM	0.977975	0.194833

Time based Details(sec)

Processing Time	
Embedding Time	1.37688
Retrieval Time	1.0944

Figure 6. Sample GUI for the watermark process

Figure 7 demonstrates the transaction of a new block in the blockchain network.



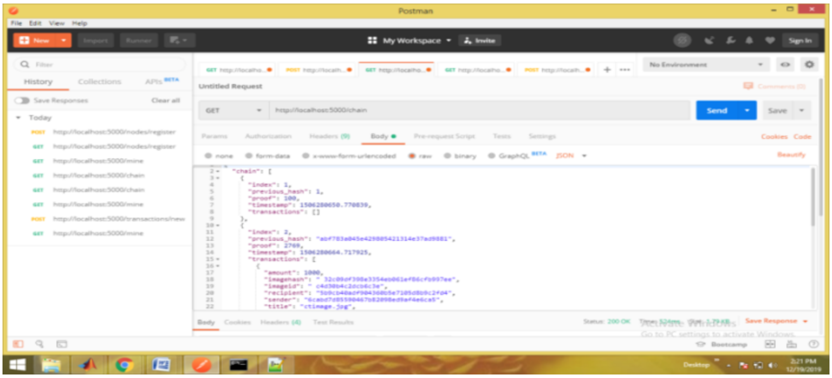
POST http://localhost:5000/transactions/new

```
{
        "amount": 1,
        "imagehash": " bccb638c7e2c17011d222ecba1684a08",
        "imageid": " c2eb3d0839e644d9",
        "recipient": "5b9cb40adf904360b5e7105d8b9c2fd4",
        "sender": "6cabd7d85590467b82098ed9af4e6ca5",
        "title": "nature.jpg",
        "usermailid": "Seetha21@gmail.com",
        "username": "Seetha"
    }
```

```
{
  "message": "Transaction will be added to Block 3"
}
```

Figure 7. Transaction of a new block in the blockchain network

Figure 8 shows the created full chain of the blockchain network.



GET http://localhost:5000/chain

```
  "chain": [
    {
      "index": 1,
      "previous_hash": 1,
      "proof": 100,
      "timestamp": 1506280650.770839,
      "transactions": []
    },
    {
      "index": 2,
      "previous_hash": "abf783a045e42980542131 4e37ad9881",
      "proof": 2769,
      "timestamp": 1506280664.717925,
      "transactions": [
        {
          "amount": 1000,
          "imagehash": " 32c09df398e3354eb061ef86cfb097ee",
          "imageid": " c4d30b4c2dcb6c3e",
          "recipient": "5b9cb40adf904360b5e7105d8b9c2fd4",
          "sender": "6cabd7d85590467b82098ed9af4e6ca5",
          "title": "ctimage.jpg",
```

Figure 8. Created blockchain

5. Conclusion and Future work

This system uses a digital watermark, Hash code, blockchain to provide a transparent, efficient and copyright protection of user’s data. The proposed system improves the robustness and security of the embedded and extracted image. The blockchain offers transparent, accurate and efficient transactions. The hash method is an effective way of preserving the more accurate record of information. The major advantage of the blockchain is in case any of the intruders attack the blockchain data they cannot be able to get back any records. DRM provides the ability for the content owner to distribute their content in a secured manner to the authorized recipients, which gives them control over the whole distribution chain. The blockchain DRM system recorded the whole transaction information. So the data will not be leaked and lost. In future, the data will be extracted from the blockchain repository InterPlanetary File System (IPFS).

References

[1] Harshini V M, Shreevani Danai, Usha H R, Manjunath R Kounte, "Health Record Management through Blockchain Technology", Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019), IEEE Xplore Part Number: CFP19J32-ART; ISBN: 978-1-5386-9439-8/19/$31.00 © IEEE 2019.

[2] Yang Lu, "The Blockchain: State-of-the-Art and Research Challenges", Journal of Industrial Information Integration, doi: https://doi.org/10.1016/j.jii.2019.04.002, 2019.

[3] Ma Zhaofeng , Huang Weihua and Gao Hongmin, "A new blockchain-based trusted DRM scheme for built-in content protection", EURASIP Journal on Image and Video Processing, https://doi.org/10.1186/s13640-018-0327-1, 2018

[4] MENG Zhaoxiong, Morizumi Tetsuya, Miyata Sumiko, Kinoshita Hirotsugu, "Design scheme of copyright management system based on digital watermarking and blockchain", 42nd IEEE International Conference on Computer Software & Applications,2018, pp. 359–364

[5] Zhaofeng Ma, Ming Jiang, Hongmin Gao, Zhen Wang, "Blockchain for digital rights management", Future Generation Computer Systems, https://doi.org/10.1016/j.future.2018.07.029, 2018

[6] Larry B. de Guzman , Ariel M. Sison, Ruji P. Medina, "MD5 Secured Cryptographic Hash Value", Association for Computing Machinery. ACM ISBN 978-1-4503-6556-7/18/09, https://doi.org/10.1145/3278312.3278317, 2018.

[7] Jasmine Josep, Anu Chalil, Gawtham G Dath, "Publicly Verifiable Digital Watermarking Technique for Copyright Property Protection", Proceedings of the International Conference on Communication and Electronics Systems (ICCES), IEEE Xplore Part Number:CFP18AWO-ART; ISBN:978-1-5386-4765-3,2018.

[8] Alexander Savelyev, "Copyright in the Blockchain Era: Promises and Challenges", National Research University Higher School of Economics (HSE), Basic Research Program Working Paper, 2017.

[9] Ruzhi Xu, Lu Zhang, Huawei Zhao and Yun Peng, "Design of Network Media's Digital Rights Management Scheme Based on Blockchain Technology," IEEE 13th International Symposium on Autonomous Decentralized Systems, 2017.

[10] Jyoti Kumari and Pankaj Vyas, "Digital Image Watermarking using DWT-SVD HF Technique", International Journal of Computer Applications (0975 – 8887), Volume 163 – No 10, April 2017

[11] Zhaofeng Ma, "Digital Rights Management: Model, Technology and Application", China Communications, 14(6), pages-156-167, doi/10.1109/CC.2017.7961371, June 2017.

[12] Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman , "MedRec: Using Blockchain for Medical Data Access and Permission Management", 2nd International Conference on Open and Big Data,2016, 978-1-5090-4054-4/16 $31.00 © 2016 IEEE DOI 10.1109/OBD.2016.11

[13] Hussain Nyeem, Wageeh Boles and Colin Boyd, "Digital image watermarking: its formal model, fundamental properties and possible attacks", Springer Open Access Journal. EURASIP Journal on Advances in Signal Processing, http://asp.eurasipjournals.com/content/2014/1/135, 2014

[14] Zhenqi and Lisha Cao, "Implementation and Comparison of Two Hash Algorithms", International Conference on Computational and Information Sciences,doi:10.1109/ICCIS.2013.195,2013.

[15] Sunesh, Harish Kumar, "Watermark Attacks and Applications in Watermarking", Department of Computer Science & Applications, CDLU, Sirsa, Haryana. National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC), Proceedings published in International Journal of Computer Applications® (IJCA), 2011.

[16] https://github.com/dvf/blockchain.