

電子透かしとブロックチェーンに基づくデジタル
画像の著作権管理システムの設計提案

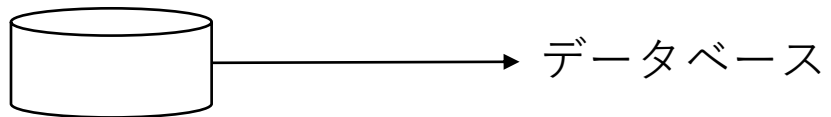
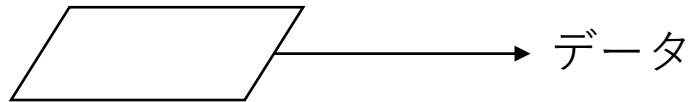
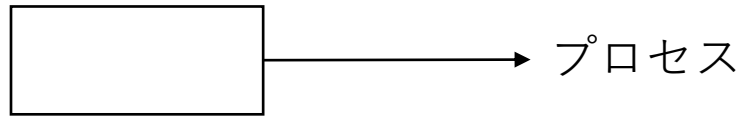
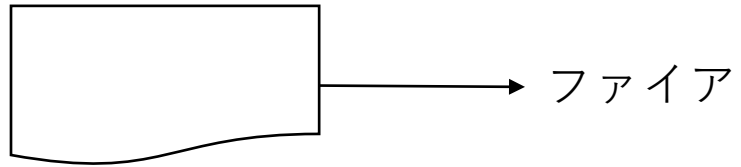
- Design proposal of digital image copyright
management system based on digital watermarking
and blockchain

名前：孟 昭雄

所属：木下研究室

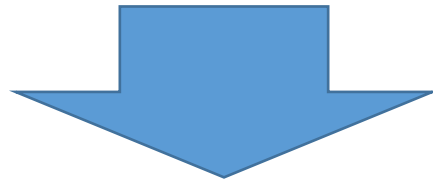
学籍番号：201770105

図表記号の凡例



研究背景

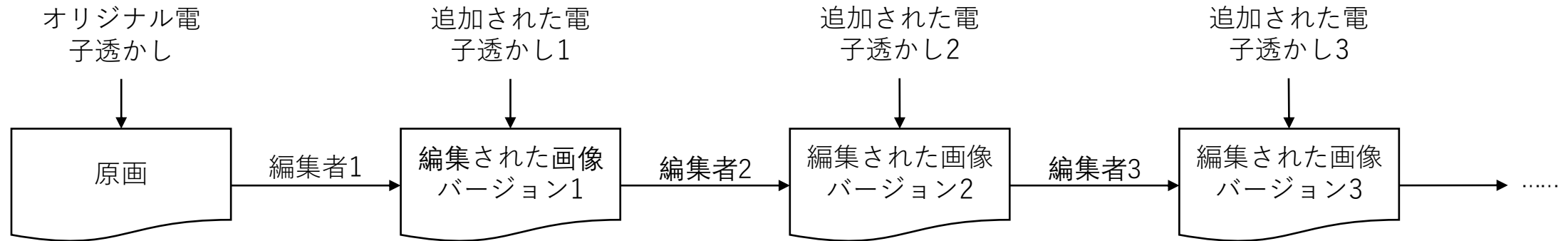
- インターネットの急速な発展は、デジタルファイルのコピー、転載、ダウンロードなどの操作をより容易にした。
- デジタル画像を編集または再作成する際には、各編集者の著作権情報と編集の順序を証明する必要がある。
- 信頼できる第三者に基づく著作権管理システムでは、著作権情報の改ざんや削除のリスクがある。



- より安全な著作権管理システムが必要である。

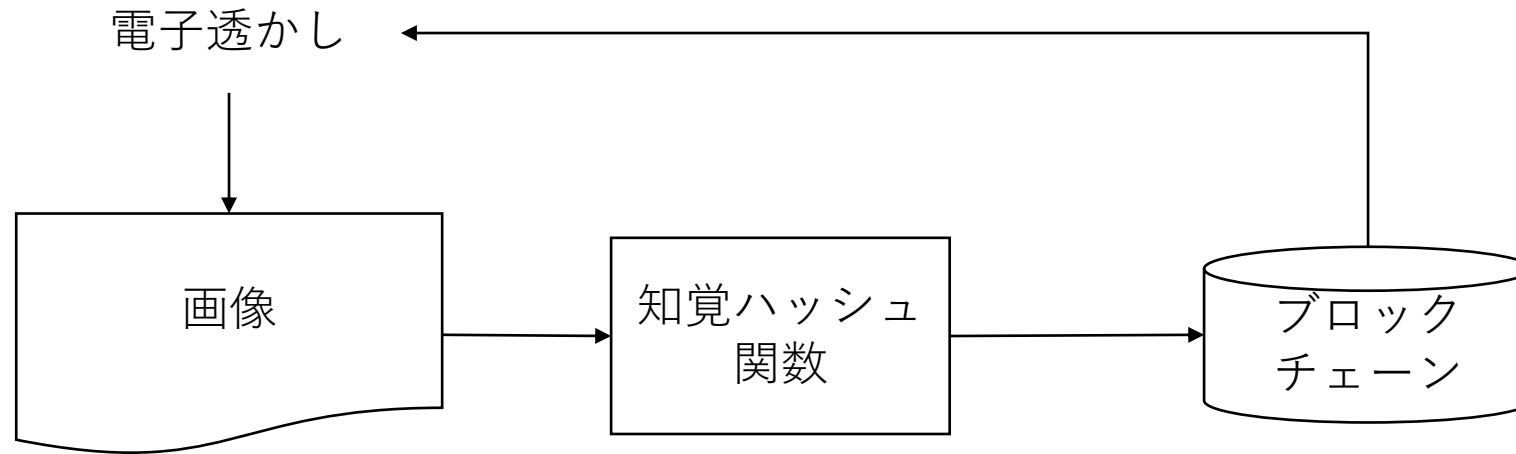
研究問題

- 原画にオリジナル電子透かしを埋め込んだ後、画像を編集するたびに、新しい電子透かしを追加する。これは電子透かしの連鎖、すなわち多重電子透かしを形成した。



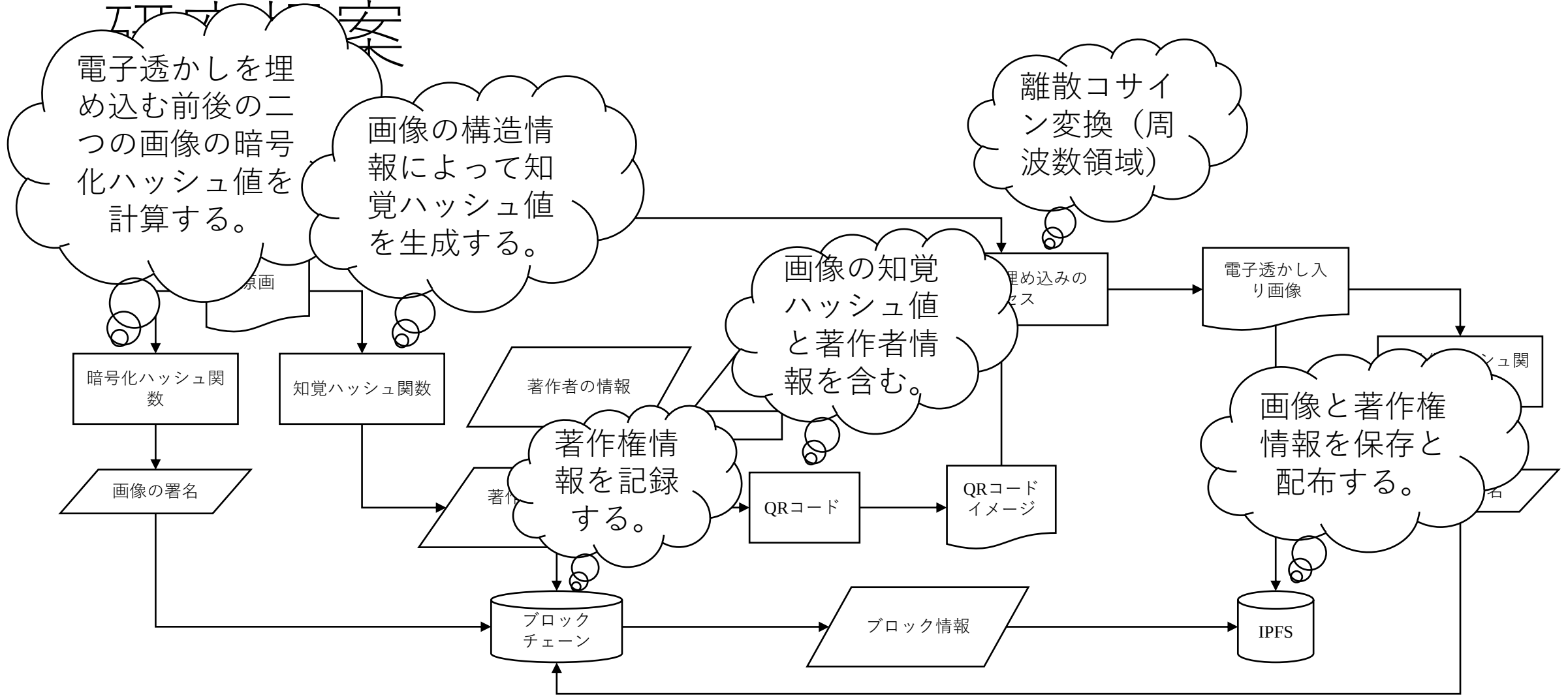
- 信頼できる第三者に依存しなく、多重電子透かしの埋め込み順序を証明する。
- デジタルファイルのハッシュを計算する際には、加工、符号化などの通常の操作または不審者からの攻撃に一定の耐性がある。

システムのオリジナリティ



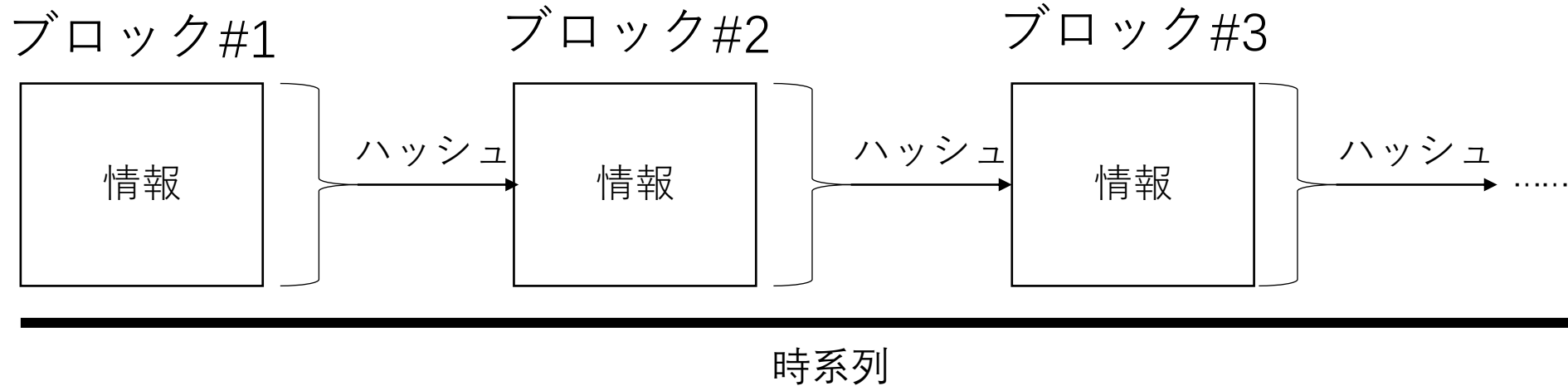
- ブロックチェーンを使用して、画像の編集・加工した履歴を記録する。
- 知覚ハッシュ関数を使用して、透かし情報とするハッシュを計算する。

研究案



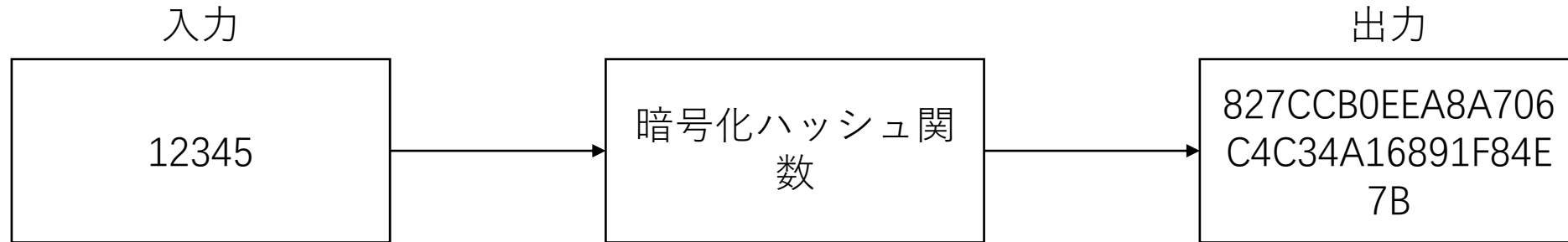
ブロックチェーン

リンクされたブロック



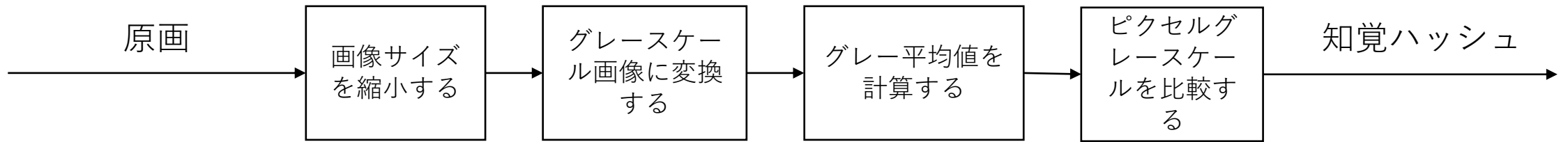
- 分散化
- 改ざん、偽造、削除などの操作が容易ではない。
- シーケンス関係を持つイベントを記録できる。
- ブロックチェーンは著作権情報を記録するために使用される。

暗号化ハッシュ関数



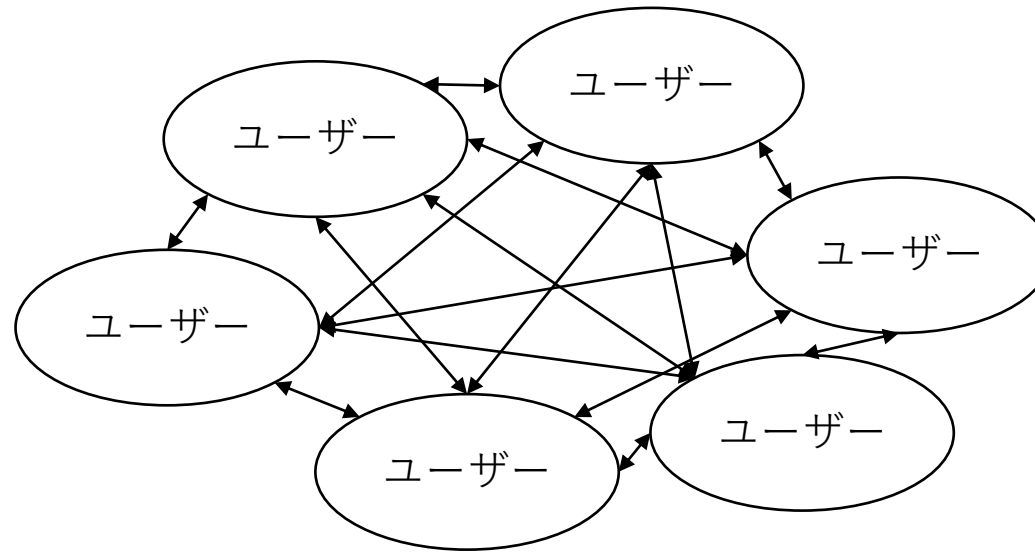
- 一方向性, 敏感性
- 暗号ハッシュ関数は元のデータのダイジェストをデジタル署名として計算するために使用される。
- 原画と電子透かし入り画像は冗長性が大きいいため, 加工や符号化によって視覚的に見た目が変わらなくても数値データとしては異なるため, 暗号ハッシュ関数は適用できない。

知覚ハッシュ関数



- 操作にロバスト，改ざんに敏感
- 知覚ハッシュ関数は処理やコーディングに対して耐性のあるダイジェストを計算するために使用される。
- このハッシュ関数は視覚的知覚に関連している。つまり，外観が変わらない限り，値は変わらない。

IPFS (InterPlanetary File System)



- 分散ファイルシステム、P2P、永久、共有
- IPFSは電子透かし入り画像と著作権情報の保存と配布に使用される。
- IPFSはブロックチェーンの容量制限を解決できる。

ハッシュの計算

imagehash=
2db16cce610bf777a8a0c316a55ca041

原画の暗号化ハッシュ値

- 電子透かしを埋め込んだ後の画像の変化を証明するために、暗号化ハッシュ関数を使って原画を計算する。

imageID=
6e0e9edaccc85a1c

原画の知覚ハッシュ値

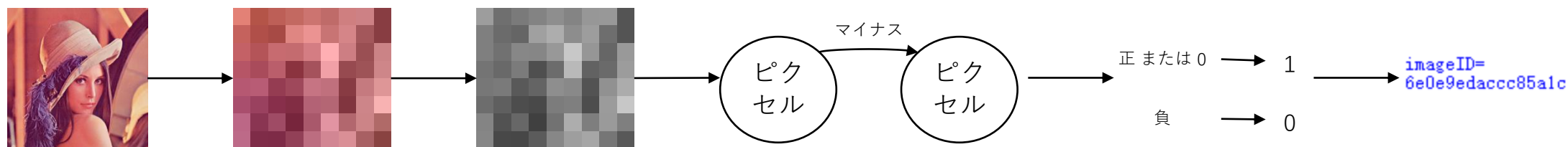
- 原画のIDとして原画の知覚ハッシュを計算する。

四つの知覚ハッシュアルゴリズムのテスト結果

四つのアルゴリズムのテスト結果

ハミング 距離 イメージ	アルゴリズム	平均ハッシュアルゴリズム	差分ハッシュアルゴリズム	知覚ハッシュアルゴリズム	ウェーブレットハッシュアルゴリズム
電子透かし入り		0	0	0	0
ノイズ		0	0	0	0
フィルタ		0	0	0	0
圧縮		3	0	0	0
切る		13	1	12	14
回転		14	7	12	14

差分ハッシュアルゴリズムの計算プロセス



差分ハッシュアルゴリズムの計算プロセス

- 画像を 9×8 のサイズに縮小し、合計72個のピクセルにする。
- 色を削除し、カラー画像をグレースケール画像に変換する。
- 隣接する二つの画素が減算され（行内の左の画素から右の画素を引く）、八つの異なる差分値が得られ、合計64個の差分値が得られる。
- 差分値が処理される。正または0の場合は1を取り、負の場合は0を取る。
- 64個の結果を組み合わせてハッシュ値を取得する。

取引の追加

```
{  
  "name": "Meng Zhaoxiong",  
  "mailaddress": "mengzhaoxiong1899@gmail.com",  
  "imageID": "6e0e9edaccc85a1c",  
  "imagehash": "2db16cce610bf777a8a0c316a55ca041",  
  "title": "lena.jpg",  
  "sender": "6cabd7d85590467b82098ed9af4e6ca5",  
  "recipient": "d10d92b01429444e919897eb5221e813",  
  "amount": 1  
}
```

取引情報をブロックに追加する

- ハッシュ値と著作者情報を取引情報としてブロックに追加する。

ブロックの生成

```
{
  "index": 2,
  "message": "New Block Forged",
  "previous_hash": "38f811e2c1849cb073fea854c3c1efba375014e26b40b7810757c26e3e3cd89e",
  "proof": 35293,
  "transactions": [
    {
      "amount": 1,
      "imageID": "6e0e9edaccc85a1c",
      "imagehash": "2db16cce610bf777a8a0c316a55ca041",
      "mailaddress": "mengzhaoxiong1899@gmail.com",
      "name": "Meng Zhaoxiong",
      "recipient": "d10d92b01429444e919897eb5221e813",
      "sender": "6cabd7d85590467b82098ed9af4e6ca5",
      "title": "lena.jpg"
    },
    {
      "amount": 1,
      "imageID": "NONE",
      "imagehash": "NONE",
      "mailaddress": "NONE",
      "name": "NONE",
      "recipient": "2d36633890b249f6a237a56cea8e3278",
      "sender": "0",
      "title": "NONE"
    }
  ]
}
```

マイニングして新しいブロックを生成する

- ブロックチェーンネットワーク内のノードはマイニングによって新しいブロックを生成する。

ブロックチェーンの生成

```
{
  "chain": [
    {
      "index": 1,
      "previous_hash": "1",
      "proof": 100,
      "timestamp": 1521601744.2542307,
      "transactions": []
    },
    {
      "index": 2,
      "previous_hash": "38f811e2c1849cb073fea854c3c1efba375014e26b40b7810757c26e3ecd89e",
      "proof": 35293,
      "timestamp": 1521601790.5997922,
      "transactions": [
        {
          "amount": 1,
          "imageID": "6e0e9edaccc85a1c",
          "imagehash": "2db16cce610bf777a8a0c316a55ca041",
          "mailaddress": "mengzhaoxiong1899@gmail.com",
          "name": "Meng Zhaoxiong",
          "recipient": "d10d92b01429444e919897eb5221e813",
          "sender": "6cabd7d85590467b82098ed9af4e6ca5",
          "title": "lena.jpg"
        },
        {
          "amount": 1,
          "imageID": "NONE",
          "imagehash": "NONE",
          "mailaddress": "NONE",

```

正当なブロックチェーン

- 他のノードによって確認された後、新しく生成されたブロックは正当なブロックチェーンに追加された。

QRコードイメージの生成



元のQRコードイメージ

```
import qrcode
qr = qrcode.QRCode(
    version=1,
    error_correction=qrcode.constants.ERROR_CORRECT_M,
    box_size=2,
    border=4,
)
qr.add_data(
    'Meng Zhaoxiong\n'
    'mengzhaoxiong1899@gmail.com\n'
    '6e0e9edaccc85a1c\n'
)
qr.make(fit=True)
img = qr.make_image()
img.save('mark.png')
```

QRコード画像の内容とパラメータ

- 知覚ハッシュ値と著作者情報を含むQRコード画像を生成する。

電子透かしの埋め込みと抽出



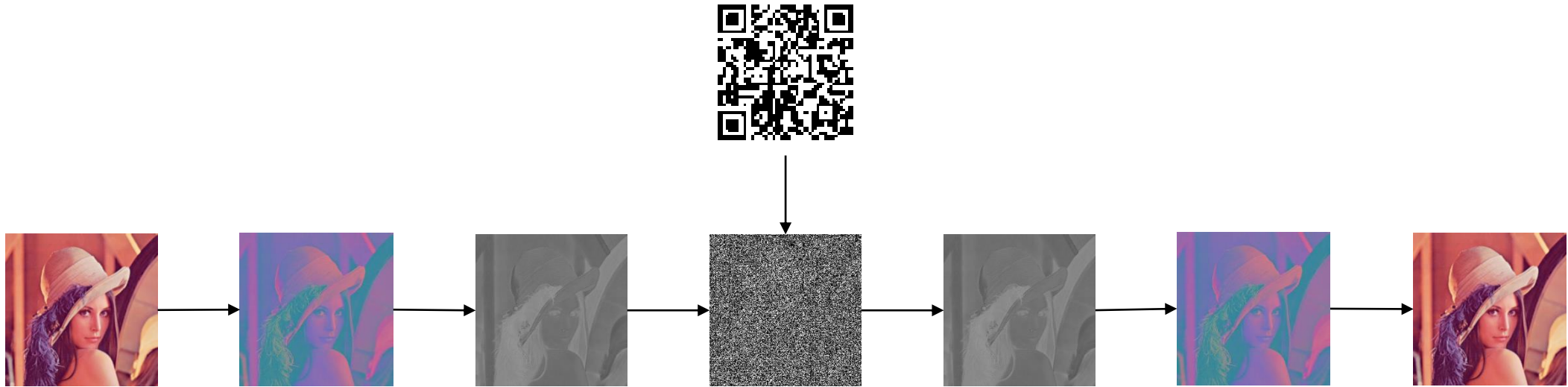
imagehash_marked=
83788acc3c01651a7148a6b05ef329ae

電子透かし入り画像の暗号化ハッシュ値

電子透かし入り画像 抽出されたQRコードイメージ

- DCTを使用して原画を空間領域から周波数領域に変換し，QRコードイメージを原画の周波数領域に埋め込み，次にIDCTを使用して原画を周波数領域から空間領域に変換する。
- 周波数領域電子透かしアルゴリズムは強い攻撃防止能力を持ち，著作権保護のための電子透かし技術に適している。
- 前と同じように，電子透かし入り画像を計算するために同じ暗号化ハッシュ関数を使用する。二つの画像は同じように見えたが，ハッシュはもう変わった。

電子透かしの埋め込みプロセス



電子透かしの埋め込みプロセス

- RGBモードをYUVモードに変換する。
- 電子透かしはカラーレイヤーUに埋め込まれる。
- Uレイヤーに対して二次元離散コサイン変換を行う。
- 二つの異なる乱数列を生成してスケールファクタを設定する。
- 二次元逆離散コサイン変換を実行して、空間ドメインを復元する。
- Uレイヤー、Yレイヤー、Vレイヤーを組み合わせる。
- YUVモードをRGBモードに変換する。

画像ファイルと著作権情報のアップロード

```
C:\学習\論文\programming(go)\go-ipfs>ipfs daemon
Initializing daemon...
Swarm listening on /ip4/127.0.0.1/tcp/4001
Swarm listening on /ip4/169.254.147.5/tcp/4001
Swarm listening on /ip4/169.254.174.225/tcp/4001
Swarm listening on /ip4/169.254.186.32/tcp/4001
Swarm listening on /ip4/192.168.150.73/tcp/4001
Swarm listening on /ip6:::1/tcp/4001
Swarm listening on /p2p-circuit/ipfs/QmYYmXLFCmyG4g5kc8K9BAUw257aJ6MPGLAFE9E7afpbW2
Swarm announcing /ip4/127.0.0.1/tcp/4001
Swarm announcing /ip4/169.254.147.5/tcp/4001
Swarm announcing /ip4/169.254.174.225/tcp/4001
Swarm announcing /ip4/169.254.186.32/tcp/4001
Swarm announcing /ip4/192.168.150.73/tcp/4001
Swarm announcing /ip6:::1/tcp/4001
API server listening on /ip4/127.0.0.1/tcp/5001
Gateway (readonly) server listening on /ip4/127.0.0.1/tcp/8080
Daemon is ready
```

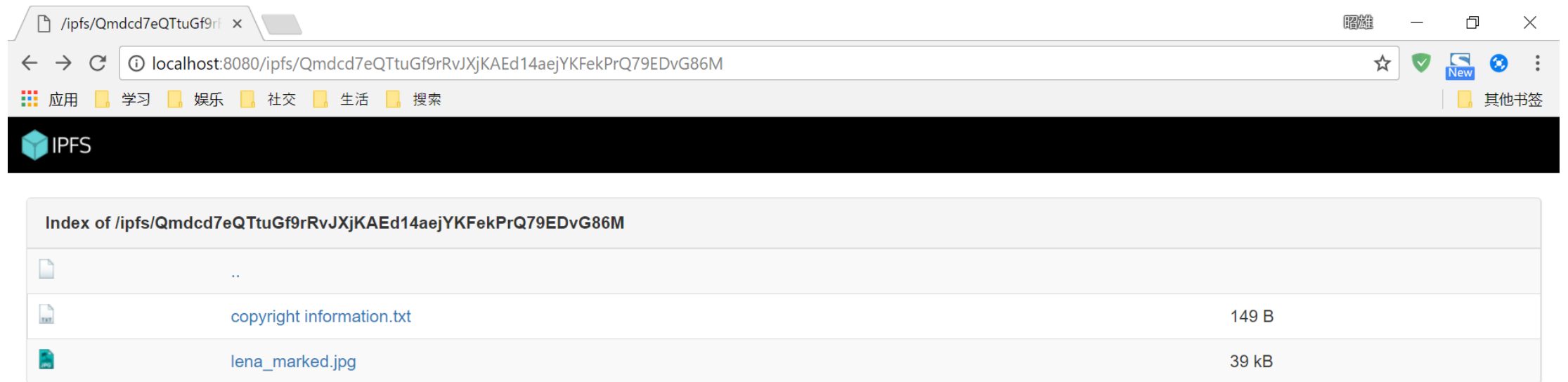
- IPFS Webサイトで提供されているgo-ipfsソフトウェアを使用する。
- 電子透かし入り画像と著作権情報のファイルを含むフォルダをIPFSネットワークにアップロードする。

IPFSの実行

```
C:\学習\論文\programming(go)\go-ipfs>ipfs add -r lena
172 B / 37.80 KB [>-----] 0.44% 0s
added QmTpzWxtBNhbf13inzyU9ydt4QQSRbTBtx9J3m1pd7U1hN lena/copyright information.txt
37.80 KB / 37.80 KB [=====] 100.00% 0s
added QmXoqFtd9QLQPhe6nmpotmky7QwJLzSQWPz7Q82mccCzG5 lena/lena_marked.jpg
added QmXik2CN6GsSvxudKxoXdXGLpuAaKiuzkrLDuAg2chc8T2 lena
```

電子透かし入り画像と著作権情報のアップロード

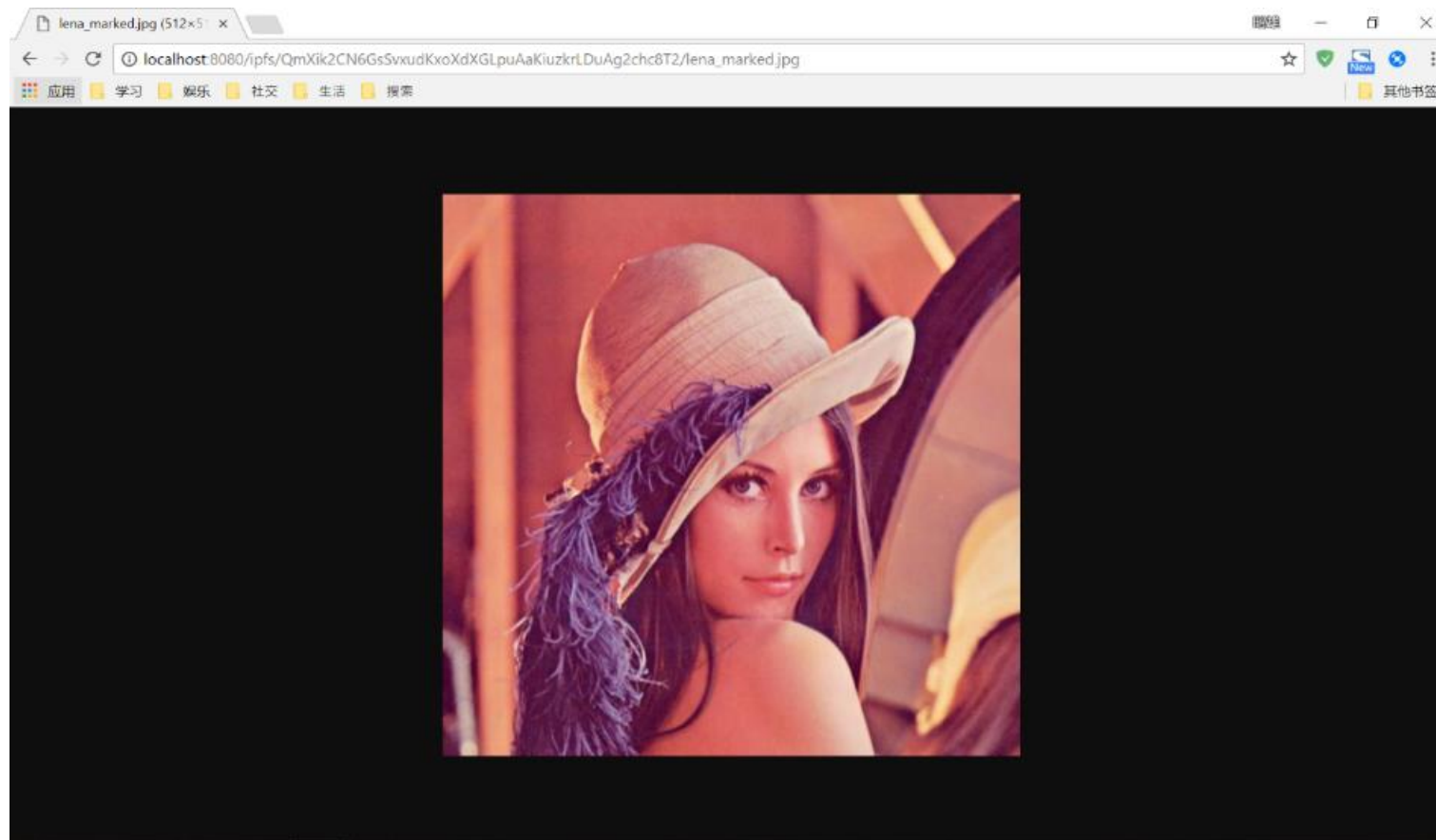
画像と著作権情報の表示



ファイルの表示

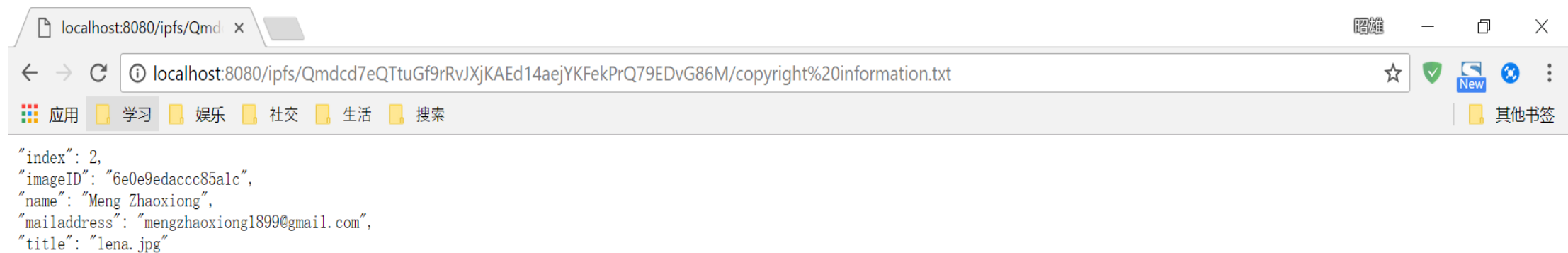
- ブラウザーを使用して電子透かし入り画像と著作権情報を表示する。

電子透かし入り画像の表示



電子透かし入り画像の表示

著作権情報の表示

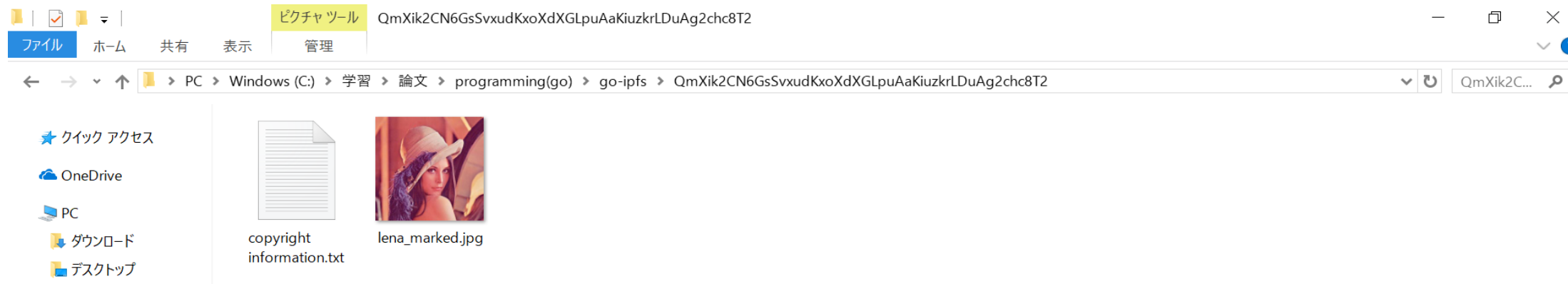


著作権情報の表示

画像ファイルと著作権情報のダウンロード

```
C:\学習\論文\programming(go)\go-ipfs>ipfs get QmXik2CN6GsSvxudKxoXdXGLpuAaKiuzkrLDuAg2chc8T2
Saving file(s) to QmXik2CN6GsSvxudKxoXdXGLpuAaKiuzkrLDuAg2chc8T2
37.95 KB / 37.95 KB [=====] 100.00% 0s
```

ファイルのダウンロード



ダウンロードされたファイル

- 電子透かし入り画像と著作権情報のファイルをダウンロードする。

まとめ

- 画像を編集・加工した履歴のブロックチェーンによって，信頼できる第三者に依存しなく，順序関係が証明でき，著作権が護られる手法とシステムを提案した。
- 画像の編集・加工に耐性のある知覚ハッシュ関数を使用して，電子透かしの連鎖が破壊されない手法とシステムを提案した。
- ブロックチェーンは著作権情報のセキュリティを保証した，電子透かしは流通中のデジタルファイルのセキュリティを保証した。
- 知覚ハッシュ関数、暗号化ハッシュ関数、QR コード、IPFSなどの技術でシステムの機能を整備して，著作権に二重の保護を加えた。

今後の課題

- ブロックチェーンをコアとして、深層学習、ハッシュ、分散ストレージなどの技術と組み合わせて、著作権管理システムの設計をさらに検討する。

学会発表

- MENG Zhaoxiong, MORIZUMI Tetsuya, MIYATA Sumiko, KINOSHITA Hirotsugu, “Design scheme of copyright management system based on digital watermarking and blockchain,” 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), volume:02, pages:359-364, 23-27 July 2018.