Computer Security Symposium 2017
23 - 25 October 2017

画像電子透かしに対する機械学習アルゴリズムの性能評価

佐久間 稜[†1] 姜 玄浩[†2] 岩村 惠市[†1] 越前 功[†3]

概要：電子透かしはコンテンツに情報を埋め込む技術である．我々は，切り抜き攻撃に耐性のある機械学習を用いた電子透かしを提案している．画像全体に格子状にマーカーを埋め込み，機械学習により得られたモデルを利用し 2 値化することで，マーカーを抽出し，切り抜き攻撃に対して同期をとることができる．我々の提案手法は IHC 委員会の評価基準 Ver.3 を達成した。その手法では Support Vector Regression という機械学習アルゴリズムを用いたが、本稿では様々な機械学習アルゴリズムに対する評価を追加して示す。

キーワード：電子透かし,機械学習,画像

Digital Image Watermarking Focused on Various Machine Learning Techniques

Ryo Sakuma[†1] Hyunho Kang[†2] Keiichi Iwamura[†1] Isao Echizen[†3]

Abstract: Digital watermarking is a technique used for embedding information in digital content. We have already proposed a digital watermarking scheme with cropping tolerance based on machine learning. The synchronization marker is embedded in a lattice-shape in the low frequency domain. Binarization processing is performed on the watermarked image to find the lattice-shaped marker and synchronize against cropping. As a result, we have achieved sufficient image quality to satisfy the IHC evaluation criteria Ver.3. In that method, we used machine learning algorithm called Support Vector Regression. In this paper, we additionally show evaluation on various machine learning algorithms.

Keywords: Digital Watermarking, Machine Learning, Image

1. はじめに

近年，画像や音声などがデジタル化され，デジタルコンテンツを様々な端末から手軽に利用できるようになっている. これらのデジタルコンテンツを劣化なしに複製したり，インターネット上で配布したりすることは容易である．そのためデジタルコンテンツの不正な取り扱いによる著作権侵害などが深刻な問題となっている．そこで著作権保護のため，デジタルコンテンツに著作権情報やコピー制御情報を人間には知覚できないような方法で埋め込む電子透かし技術が研究されている．

電子透かしは品質，耐性，容量の 3 項目で評価されることが多いが，近年まで明確な評価基準は定められていなかった．そこで情報ハイディングおよびその評価基準委員会(IHC 委員会)[1]が設立され，画像・音響・映像についての具体的な評価基準を定め，その基準を達成する電子透かし方式[2-4]を募集し，コンテストを行い，その結果に応じて評価基準をより厳しいものへと更新していくことを行っている．

IHC 委員会の最新の評価基準を達成するために，我々は機械学習[5][6]に着目した. 機械学習とは人間が自然に行う学習の過程をコンピュータ上で実現しようとする技術のことである．原画像，透かし入り画像，攻撃を受けた画像から不変の特徴を見つけ，機械学習させる．それにより得られた機械学習モデルを用いることで，我々は新しい電子透かしを提案しようとしている．

機械学習を用いた電子透かしはこれまで非常に少数の研究者によって研究されてきた[7-10]．機械学習を用いた電子透かしを最初に提案したのは Chun-hua Li らである[7]. ある画素とその周りの画素の関係性を機械学習させ，機械学習モデルを形成する．埋め込みに用いる画素の画素値をその周りの画素から機械学習モデルによって予測された画素値を基準として操作・比較することによって透かしを埋め込む．機械学習モデルの高い学習能力と一般化能力により，彼らの手法は実現している．しかしながら，機械学習を用いた電子透かしには，切り抜き，スケーリング，回転などの非同期攻撃に対して，耐性がほとんど無い問題がある．

そこで我々は，切り抜き攻撃に対して耐性のある機械学習を用いた電子透かしを提案した[11]．画像の輝度領域に Wavelet 変換[12][13]を施し，低周波領域を得る．得られた低周波領域を 3×3 のブロックに分割する. 低周波領域から

†1 東京理科大学大学院
Tokyo University of Science
†2 東京工業高等専門学校
National Institute of Technology
†3 国立情報学研究所
National Institute of Informatics

選ばれたブロックの中心の係数とその周りの係数の関係性を機械学習させ，機械学習モデルを形成する．埋め込みに用いるブロックの中心の係数を，その周りの係数から機械学習モデルによって予測された係数を基準として操作・比較することによって，透かしを埋め込む．また，透かしに対して，誤り訂正符号の一つとしてよく知られる BCH 符号[14][15]を用いることで，圧縮耐性を高めた．加えて，低周波領域に格子状に同期用マーカーを埋め込む．透かし入り画像を 2 値化処理することによって，その同期用マーカーを見つけることができるようになる．結果として，切り抜き攻撃に対しても耐性のある電子透かしを実現した.また，提案手法を IHC 委員会の定める評価基準 Ver.3 によって評価を行い，達成した．

本稿では，前述の評価に加えて、提案手法の機械学習アルゴリズムに関して評価を行った。

本論文の構成は以下の通りである．2 章で関連研究について説明し，3 章で提案手法，4 章で評価，5 章でまとめを示す．

2. 関連研究

関連研究について示す．また，本研究で用いた基本的な技術についてもこの章で述べる．

2.1 関連手法[7]

機械学習を用いた電子透かしは，非常に少数の研究者によって研究されてきた．機械学習を用いた電子透かしを最初に提案したのは Chun-hua Li らである．ある画素とその周りの画素の関係性を機械学習させ，機械学習モデルを形成する．埋め込みに用いる画素の画素値を，その周りの画素から機械学習モデルによって予測された画素値を基準として，操作・比較することによって，透かしを埋め込む．機械学習モデルの高い学習能力と一般化能力により，彼らの手法は実現している．彼らが提案した手法を以下に詳細に説明する．

2.1.1 機械学習モデル形成

画像 I を 3×3 の大きさのブロックに分割する．学習に用いるブロックを鍵k_1によって選定する．選定されたブロックの周囲の 8 つの画素から，中心の画素を予測する機械学習モデルを形成するために，訓練用データセットΩを作成する．

$$\Omega = \left\{ \begin{matrix} I_{i_t-1,j_t-1}, I_{i_t-1,j_t}, I_{i_t-1,j_t+1}, I_{i_t,j_t-1}, I_{i_t,j_t+1}, \\ I_{i_t+1,j_t-1}, I_{i_t+1,j_t}, I_{i_t+1,j_t+1}, I_{i_t,j_t} \end{matrix} \right\}_{t=1\dots k} \quad (1)$$
$$= \{D_t, r_t\}_{t=1\dots k}$$

ここで k は学習に用いるブロックの個数である．r_tは学習に用いるブロックの中心の画素であり，機械学習における出力となる．D_tは学習に用いるブロックの周りの 8 つの画素であり，機械学習における入力となる．このデータセットを Support Vector Regression(SVR)を用いて機械学習させ，学習モデル *F* を得る．

2.1.2 透かし埋め込み

画像 I から，埋め込みに用いるブロックを鍵k_2によって選定する．選定されたブロックの周りの 8 つの画素を入力として，学習モデル *F* に代入する．出力として得られた値をV_{ρ_t}とする．この値を用いてブロックの中心の画素I_{ρ_t}を以下の式に従って操作し，透かしを埋め込む．

$$I_{\rho_t} = \begin{cases} \max(I_{\rho_t}, V_{\rho_t} + \alpha) & \text{if } w_t = 1 \\ \min(I_{\rho_t}, V_{\rho_t} - \alpha) & \text{otherwise} \end{cases} \quad (2)$$
$$(t = 1 \dots n)$$

ここでαは埋め込み強度，w_tは透かし情報，ρ_tは選定されたブロックのインデックス，n は埋め込むビット数である．

2.1.3 透かし抽出

画像$\bar{I}$から，透かしを埋め込んだブロックを鍵k_2によって選定する．選定されたブロックの周りの 8 つの画素を入力として学習モデル *F* に代入する．出力として得られた値を$\overline{V_{\rho_t}}$とする．この値とブロックの中心の画素$\overline{I_{\rho_t}}$を比較することによって透かしを抽出する．

$$\overline{w_t} = \begin{cases} 1 & \text{if } \overline{I_{\rho_t}} > \overline{V_{\rho_t}} \\ 0 & \text{otherwise} \end{cases} \quad (t = 1 \dots n) \quad (3)$$

ここで$\overline{w_t}$は抽出した透かし情報，ρ_tは選定されたブロックのインデックス，n は埋め込まれたビット数である．

2.1.4 問題点

彼らが提案した機械学習を用いた電子透かしには，切り抜き，スケーリング，回転などの非同期攻撃に対して，耐性がほとんど無い問題がある．これを解決するために，我々は機械学習に着目した．

2.2 BCH 符号[14][15]

BCH 符号は Hocquenghem，Bose，Ray-Chaudhuri らによって考案された誤り訂正符号のうちの一つである．GF(2)上のシンボルのガロア配列としてあらわされるメッセージを符号化する．メッセージ長と符号長ごとに，誤り訂正能力が決まっている．提案手法では，透かしを BCH 符号によって符号化することで耐性を向上させている．

2.3 Wavelet 変換[12][13]

Wavelet 変換とは信号周波数が経時的に変化する場合の信号解析を実行するための数学的手法であり，画像の特性を解析する手段として有効なものである．画像に対して 1 段階の Wavelet 変換を施すと低周波成分と 3 つの高周波成分を得ることができる．この中でも低周波成分は他の成分と比べ，画像処理を施されても変化しにくい．提案手法では，低周波成分を用いることによって耐性を向上させている．

2.4 機械学習[5][6]

機械学習とは，人間の学習過程をコンピュータ上で実現しようとする技術のことである．出力データは入力データによって決まるものとする．トレーニングデータによって機械学習モデルを形成し，新たに入力されたデータの出力を予測する．

我々は，原画像，透かし入り画像，攻撃された画像から，不変の特徴を見つけ出し，その特徴を学習させることによって形成される機械学習モデルを使用することによって，新しい電子透かしを提案しようとしている．

3. 提案手法

3.1 切り抜き攻撃に対する同期方法

ここで，我々の提案手法における切り抜き攻撃に対する同期方法について詳細に示す．画像の輝度値の低周波領域に同期マーカーを埋め込む．この同期マーカーは，低周波領域に透かし情報として「1」か「0」を連続的に格子状に埋め込んだものである．図 1 は原画像に対して同期マーカーを埋め込んだものである．抽出時，このマーカーを埋め込まれた画像を 2 値化処理することによって，マーカーを検出する．この 2 値化処理は，関連手法の抽出操作を画像全体に施すことによるものである．図 2 は埋め込まれた画像に対して，2 値化処理を施したものである．この 2 値化画像において，格子状の同期マーカーを見つけることは容易である．

図 3 はマーカーを埋め込まれた画像から一部分を切り抜いた画像である．どちらも，格子状に埋め込まれた同期マーカーを見つけることができる．

我々は，この同期マーカーと 2 値化処理によって，切り抜き攻撃に対しても耐性のある電子透かしを実現した．また，この同期手法は，回転やスケーリングなどの攻撃に対しても有効であると期待される．

図 1　同期マーカー埋め込み画像

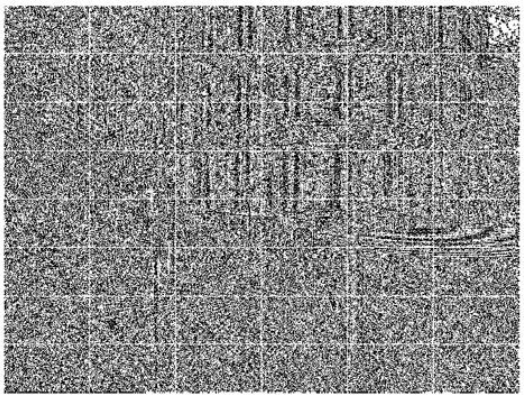

図 2　2 値化された画像

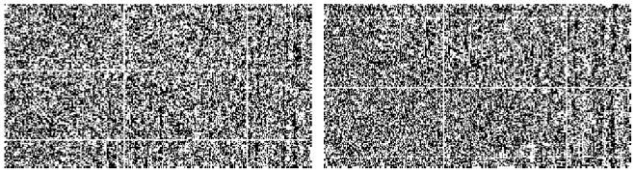

図 3　切り抜き攻撃された画像

3.2 透かしの埋め込み

提案手法の透かし埋め込みの詳細についてここで説明する．Cはサイズ$m \times n$の原画像で，WはLビットの透かし情報である．

3.2.1 透かしの符号化

透かしWを BCH 符号によって符号化する．BCH 符号における訂正能力 Tは符号長 Nとメッセージ長 Kにより決まる．符号化された透かし$W1(L1$ビット)は以下の通りである．

$$W1 = \{W1_t | 1 \le t \le L1\} \tag{4}$$

3.2.2 学習・埋め込みに用いる領域の取得

原画像Cは RGB 領域から YCbCr 領域に変換され，輝度領域Yを得る．

$$Y = \{Y_{i,j} | 1 \le i \le m, 1 \le j \le n\} \tag{5}$$

輝度領域に 1 段階のウェーブレット変換を行い，低周波領域LLを得る．

$$LL = \{LL_{i,j} | 1 \le i \le m/2, 1 \le j \le n/2\} \tag{6}$$

低周波領域LLは 3×3 の大きさのブロックに分割される．

3.2.3 学習モデルの形成

低周波領域LLにおいて，ある係数とその周囲の係数との関連性をモデル化するために，訓練用データセットΩとしていくつかのブロックを選定する．選ばれたブロックの中心座標は以下のようになる．

$$\rho 1_t = (i_t, j_t) \ (1 \le i_t \le m, 1 \le j_t \le n) \tag{7}$$

訓練用データセットΩは以下のように表現される．

$$D_t = \begin{Bmatrix} LL_{i_t-1,j_t-1}, LL_{i_t-1,j_t}, LL_{i_t-1,j_t+1}, \\ LL_{i_t,j_t-1}, LL_{i_t,j_t+1}, \\ LL_{i_t+1,j_t-1}, LL_{i_t+1,j_t}, LL_{i_t+1,j_t+1} \end{Bmatrix}_{t=1,\dots,k} \tag{8}$$

$$r_t = \{LL_{i_t,j_t}\}_{t=1,\dots,k} \quad (9)$$

$$\Omega = \{D_t, r_t\}_{t=1,\dots,k} \quad (10)$$

ここでkは訓練用データの数，r_tは機械学習における出力，D_tは機械学習における入力である．我々の事前の調査より，訓練用データの数が電子透かし自体に大きな影響は及ぼさないことが分かっている．それゆえ、学習に用いるブロック数をできる限り削減し，埋め込みに用いるブロックを増やすことが可能である．

今回，我々が用いる機械学習アルゴリズムは SVR である．訓練用データセットΩを，SVR を用いて学習させることにより，学習モデル F を得る．形成された学習モデル F は入力から出力を予測するものである．

$$F(x) = \sum_{t=1}^{k} (\beta_t^* - \beta_t) Ker\,(D_t, x) + b1 \quad (11)$$

ここでβはラグランジュ係数，Ker はカーネル関数，$b1$ はバイアスである．

3.2.4 透かしと同期マーカーの埋め込み

切り抜き攻撃に耐性を持たせるため，同期マーカーを埋め込む．透かし入り画像が$m'' \times n''$の大きさに切り抜かれる場合，低周波成分において透かしを埋め込める領域の大きさはa×bである．ここでaとbの範囲は$a \le m''/4$かつ$b \le n''/4$でなければならない．また、透かしを埋め込む領域の上端と左端に同期マーカーとして，「1」または「0」の情報を連続的に埋め込む．

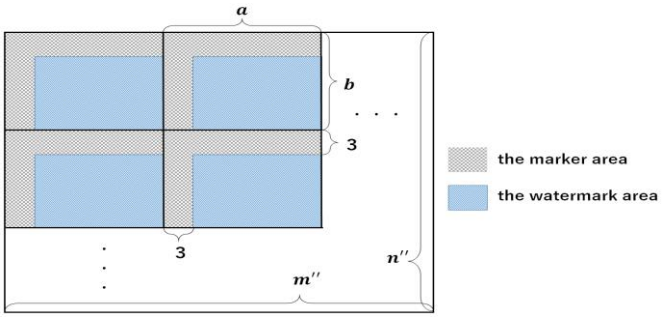

図 4　同期マーカーと透かしの埋め込み領域

符号化された透かしを埋め込むために，無作為に$L1$ブロックを選定する．選ばれたブロックの中心座標は以下の通りである．

$$\rho 2_t = (i_t, j_t) \quad (1 \le i_t \le a, 1 \le j_t \le b) \quad (12)$$

形成された学習モデル F に代入するためのデータセットΦを以下のように作成する．

$$\Phi = \{D_t\}_{t=1,\dots,L1} \quad (13)$$

データセットΦを学習モデル F に代入して得られた出力を$V_{\rho 2_t}$とする．以下の式に従って，選ばれたブロックの中心座標の係数を操作することによって，透かしと同期マーカーを埋め込む．

$$LL_{\rho 2_t} = \begin{cases} max(LL_{\rho 2_t}, V_{\rho 2_t} + \alpha) & if\ \ W1_t = 1 \\ min(LL_{\rho 2_t}, V_{\rho 2_t} - \alpha) & otherwise \end{cases} \quad (14)$$
$$(t = 1, \dots, L1)$$

ここでαは埋め込み強度である．αは電子透かし手法の耐性と品質を考慮して決められる．

3.2.5 透かし入り画像の取得

透かしを埋め込まれた輝度領域の低周波領域に逆ウェーブレット変換を施し，YCbCr 領域から RGB 領域に変換することによって，透かし入り画像C'を得る．

3.3 透かしの抽出

提案手法の透かし抽出の詳細についてここで説明する．透かし入り画像C'を$m'' \times n''$の大きさに切り抜いた画像をC''とする．この切り抜き画像C''から透かしを抽出する．

3.3.1 2 値化

切り抜き画像C''を RGB 領域から YCbCr 領域に変換し，輝度領域 Y''を得る．

$$Y'' = \{Y''_{i,j} | 1 \le i \le m'', 1 \le j \le n''\} \quad (15)$$

輝度領域Y''に 1 段階のウェーブレット変換を行い，低周波領域LL''を得る．

$$LL'' = \{LL''_{i,j} | 1 \le i \le m''/2, 1 \le j \le n''/2\} \quad (16)$$

低周波領域LL''は 3×3 の大きさのブロックに分割される．それらの中心座標を$\rho 3_t$とする．

$$\rho 3_t = (i_t, j_t)\ (1 \le i_t \le m''/2, 1 \le j_t \le n''/2) \quad (17)$$

埋め込みに用いられた学習モデル F を読み込む．読み込まれた学習モデル F に代入するためのデータセットΨを以下のように作成する．

$$\Psi = \{D''_t\}_{t=1,\dots,A} \quad (18)$$

ここで A は全てのブロック数である．データセットΨを学習モデル F に代入して得られた出力を$V''_{\rho 3_t}$とする．
以下の式に従って，低周波領域のブロックの中心の係数と学習モデルから得られた出力$V''_{\rho 3_t}$を比較することによって，2 値化画像B''を得る．

$$B''_{\rho 4_t} = \begin{cases} 1 & if \quad LL''_{\rho 3_t} > V''_{\rho 3_t} \\ 0 & otherwise \end{cases} \quad (t = 1, \dots, A) \quad (19)$$

ここで$\rho 4_t$は以下の通りである。

$$\rho 4_t = (i_t, j_t)\ (1 \le i_t \le m''/6, 1 \le j_t \le n''/6) \quad (20)$$

3.3.2 同期と抽出

切り抜き攻撃に対して同期を取るために，2 値化画像B''から，格子状に埋め込まれた同期マーカーの 4 つの交点を見つけ，透かしを埋め込んだ領域を得る．今回は，幾何学的手法によって 4 つの交点を見つけた．埋め込み位置$\rho 2_t$を読み込み，得られた透かしを埋め込んだ領域から透かしを抽出する．

$$W1'_t = B'''_{\rho 2_t} \quad (t = 1, \dots, L1') \quad (21)$$

最後に，得られた透かし$W1'$を BCH 符号を用いて復号することにより，透かしW'を得る．

4. 評価

4.1 IHC 委員会の定める評価基準 Ver.3[1]

ここで IHC 委員会の定める，画像に対する電子透かし技術の評価基準 Ver.3 について説明する．この評価基準を満たすためには，電子透かしは圧縮耐性と切り抜き攻撃に対する耐性が必要である．具体的な評価方法に関して以下に示す．まず，IHC 委員会によって用意された評価用画像 6 枚(図 5)に対して，10 種類の透かし(200bit)を埋め込む．透かし入り画像に対して 2 段階の圧縮・解凍を行う．1 段階目の圧縮でファイルサイズが元の透かし入り画像の 1/15 になるように，また，2 段階目の圧縮ではファイルサイズが 1/25 になるように，圧縮率を決定する．透かしの入っていない評価用画像も同様の圧縮率で圧縮する．各々の PSNR と MSSIM を算出し，電子透かしの品質に関して評価する．また，2 段階の圧縮後に解凍された透かし入り画像から，10 種類の切り抜き攻撃(表 1)を行い，切り抜いた画像から，埋め込んだ透かしを抽出する．抽出された透かしの誤り率は 0%でなければならない．

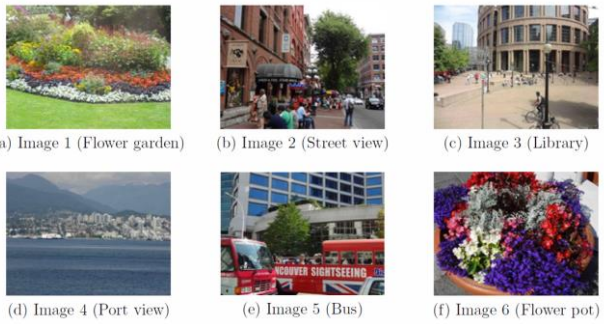

図 5　評価用画像

表 1　IHC 委員会の定める切り抜き攻撃の位置

position	(x1,y1)	(x2,y2)	(x3,y3)	(x4,y4)
1	(16,16)	(1935,16)	(1935,1095)	(16,1095)
2	(1500,16)	(3419,16)	(3419,1095)	(1500,1095)
3	(2617,16)	(4536,16)	(4536,1095)	(2617,1095)
4	(16,770)	(1935,770)	(1935,1849)	(16,1849)
5	(1500,770)	(3419,770)	(3419,1849)	(1500,1849)
6	(2617,770)	(4536,770)	(4536,1849)	(2617,1849)
7	(1344,768)	(3263,768)	(3263,1847)	(1344,1847)
8	(16,1520)	(1935,1520)	(1935,2599)	(16,2599)
9	(1500,1520)	(3419,1520)	(3419,2599)	(1500,2599)
10	(2617,1520)	(4536,1520)	(4536,2599)	(2617,2599)

4.2 提案手法の評価

IHC 委員会の定める評価基準 Ver.3 に沿って提案手法を評価した．以下に評価結果を示す．

表 2　提案手法の品質に関する評価結果

	Compression ratio		PSNR		MSSIM	
	1st coding	2nd coding	1st coding	2nd coding	1st coding	2nd coding
Image1	0.0655	0.0387	42.2507	41.1787	0.9909	0.9889
Image2	0.0649	0.0381	41.9447	42.0595	0.9801	0.9796
Image3	0.0635	0.0376	38.4955	38.6804	0.9689	0.9683
Image4	0.0665	0.0367	42.0696	40.7871	0.9869	0.9820
Image5	0.0663	0.0400	41.0439	40.0965	0.9769	0.9683
Image6	0.0659	0.0385	41.7427	41.2044	0.9859	0.9851
Average	0.0654	0.0382	41.2579	40.6678	0.9816	0.9787

表 3　提案手法の耐性に関する評価結果

	Position									
	1	2	3	4	5	6	7	8	9	10
Image1	0	0	0	0	0	0	0	0	0	0
Image2	0	0	0	0	0	0	0	0	0	0
Image3	0	0	0	0	0	0	0	0	0	0
Image4	0	0	0	0	0	0	0	0	0	0
Image5	0	0	0	0	0	0	0	0	0	0
Image6	0	0	0	0	0	0	0	0	0	0
Average	0	0	0	0	0	0	0	0	0	0

表 2 は提案手法の品質に関する評価結果である．1 段階目の圧縮率は 6.54%であり，これは評価基準に定められた 6.67%を満たしている．2 段階目の圧縮率は 3.82%であり，これも評価基準に定められた 4.00%を満たしている．また，PSNR に関して，1 段階目の圧縮後は 41.2579dB，2 段階目の圧縮後は 40.6678dB となった．30dB を越えており，基準を満たしている．

表 3 は提案手法の耐性に関する評価結果である．透かし入り画像に対し 2 段階の圧縮・解凍後，HDTV-size の切り抜き攻撃を行った際の透かしの抽出率はすべて 0%となった．

表 2，3 より，提案手法は IHC 委員会の評価基準 Ver.3 を達成したことが確認できた．

4.3 機械学習アルゴリズムごとの評価

MATLAB 上で機械学習アルゴリズムの学習精度に関しての評価を行った．アルゴリズムごとに実測値と予測値の RMSE を算出し評価した．RMSE の値が小さいほど，良い学習精度である．

$$\mathrm{RMSE} = \sqrt{\frac{1}{n}\sum_{k=1}^{n}(f_i - y_i)^2} \qquad (22)$$

ここで n はデータの数，f_iは予測値，y_iは実測値である

今回評価に用いたデータセットは、評価用画像 6 枚ごとから無作為に選定した。加えて評価用画像 6 枚すべてから無作為に選定したデータセットも用意した。データ数は各々、IHC 委員会評価基準 Ver.3 達成時に用いたデータ数と同様に 300 とした。テストはデータセットを 5 分割交差子検定し、RMSE を算出した。以下に評価結果を示す．

表 4　機械学習アルゴリズム別の学習精度

	画像1	画像2	画像3	画像4	画像5	画像6	画像1－6混在
線形回帰	1.95	1.38	1.32	1.32	1.28	1.79	1.65
交互作用線形回帰	2.36	1.82	1.63	4.15	1.49	2.94	1.94
ロバスト線形回帰	1.93	1.40	1.34	1.28	1.33	1.86	1.65
ステップワイズ線形回帰	1.95	1.38	1.32	1.36	1.28	1.79	1.65
複雑な決定木	6.62	5.60	7.15	4.85	5.96	8.22	6.37
中程度の決定木	7.97	7.45	8.64	6.27	7.97	10.67	9.04
単純な決定木	13.29	11.55	14.70	8.95	11.17	16.91	14.43
線形SVM	2.26	1.58	3.77	1.51	1.77	2.71	1.79
2次SVM	3.08	2.65	5.11	2.50	2.75	5.27	2.63
3次SVM	3.73	10.66	6.13	6.16	4.67	6.33	3.66
細かいガウスSVM	13.82	15.20	11.26	9.31	13.39	13.91	12.81
中程度のガウスSVM	4.20	6.34	5.49	3.54	6.31	5.70	4.41
粗いガウスSVM	4.39	4.59	4.75	2.82	4.54	5.08	4.41
ブースティング決定木	7.63	6.38	8.07	6.47	6.82	6.83	6.67
バギング決定木	7.93	4.79	5.01	3.35	5.09	5.28	4.25
二乗指数ガウス過程回帰	1.99	1.40	1.44	1.37	1.26	1.82	1.65
Mattern 5/2 ガウス過程回帰	1.98	1.40	1.42	1.31	1.28	1.81	1.64
指数ガウス過程回帰	2.74	2.53	2.89	1.83	2.68	3.27	2.79
有理二次ガウス過程回帰	1.99	1.40	1.44	1.35	1.26	1.82	1.65

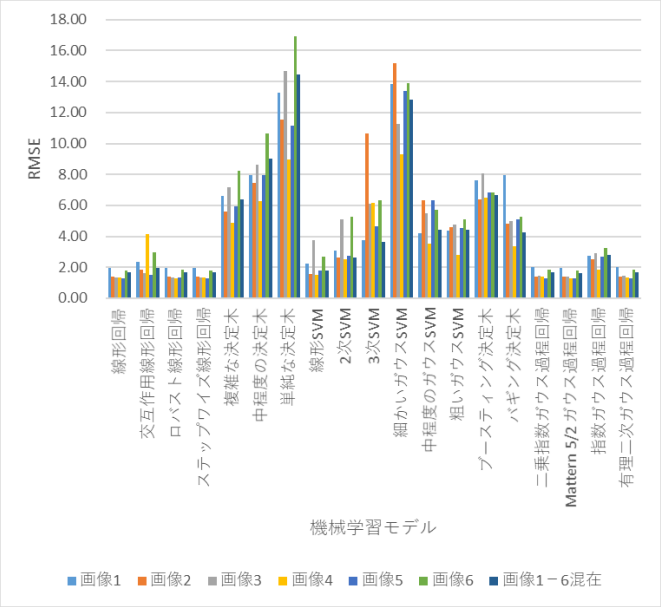

図 6　機械学習アルゴリズム別の学習精度

表 4，図 6 より，機械学習アルゴリズムの違いは，電子透かしに大きく影響を及ぼす程度のものではないことが分かる．しかし，決定木やガウス SVM などは，今回の電子透かしにおいては比較的不向きであることもわかった．

次に，提案手法を，様々な機械学習アルゴリズムを用いて MATLAB 上で実装し，評価を行った．評価には IHC 委員会の評価用画像 Image2 を使用し, IHC 委員会の評価基準に従い，用いた機械学習アルゴリズムごとに，PSNR を算出し，品質を評価した．また，機械学習アルゴリズムの訓練に用いる訓練データを 2 種類用意した．1 つは評価用画像 Image2 から無作為に 300 ブロック分, もう 1 つは評価用画像 Image1-6 の 6 枚から無作為に 300 ブロック分選定したものである．以下に評価結果を示す．

表 7　機械学習アルゴリズム別の品質評価
(訓練データ Image2 のみ)

	PSNR		MSSIM		RMSE
	1st coding	2nd coding	1st coding	2nd coding	
線形回帰	41.9354	42.0657	0.9799	0.9796	1.38
複雑な決定木	34.1747	34.1967	0.9626	0.9590	5.60
単純な決定木	32.5645	32.6270	0.9555	0.9512	11.55
線形SVM	41.9573	42.0763	0.9803	0.9798	1.58
細かいガウスSVM	31.0464	31.1194	0.9480	0.9432	15.20
指数ガウス過程回帰	35.2569	35.2014	0.9668	0.9633	2.53

表 8　機械学習アルゴリズム別の品質評価
(訓練データ Image1-6)

	PSNR		MSSIM		RMSE
	1st coding	2nd coding	1st coding	2nd coding	
線形回帰	41.9442	42.0712	0.9800	0.9796	1.65
複雑な決定木	35.3383	35.2809	0.9670	0.9635	6.37
単純な決定木	33.9961	34.0175	0.9616	0.9577	14.43
線形SVM	41.9514	42.0748	0.9801	0.9797	1.79
細かいガウスSVM	31.7756	31.8343	0.9545	0.9504	12.81
指数ガウス過程回帰	35.5209	35.4490	0.9677	0.9643	2.79

表 7，8 より，機械学習アルゴリズムの学習精度と電子透かしの品質にはある程度の相関関係があることがわかった．提案手法では，各々の画像を訓練データとして学習モデルを形成していた．今回の評価結果から，訓練データを様々な画像データとし，学習モデルを一般化しても，電子透かしの品質・耐性に大きな影響は及ぼさないことが分かった．

5.　まとめ

本稿において，我々は切り抜き耐性のある機械学習を用いた電子透かし手法を提案した．原画像の輝度の低周波領域をウェーブレット変換することで取得し，その領域に格子状に連続した透かしを同期用マーカーとして埋め込んだ．透かし入り画像に対して，機械学習を用いて 2 値化処理を施すことにより，格子状の同期用マーカーを簡単に検出することが出来るようになった．これにより，切り抜き攻撃に対して耐性のある電子透かしを実現した．また，提案手法は IHC 委員会評価基準 Ver.3 を達成し，圧縮耐性と切り抜き攻撃に対する耐性を証明した．加えて本稿では，機械学習アルゴリズムに関しての評価を行い，学習モデルの一般化の可能性が分かった．

参考文献

[1] “Information hiding and its criteria for evaluation” http://www.ieice.org/iss/emm/ihc/en/ (参照 2017/08/10)
[2] N.Hirata, M.Kawamura.. Digital watermarking method using LDPC code for clipped image. The First International Workshop on Information Hiding and its Criteria for evaluation,2014, ACMN press, pp. 25-30
[3] H.Kang, K.Iwamura.. Watermarking Based on the Difference of Discrete Cosine Transform Coefficients and Error-Correcting Code.

The First International Workshop on Information Hiding and its Criteria for evaluation,2014, ACM press, pp. 9-17
[4] H.Kang, K.Iwamura.: Information Hiding Method Using Best DCT and wavelet Coefficients and its Watermark Competition. Entropy 17, no.3, 2013, pp. 1218-1235
[5] B.Scholkopf, A.J.Smola.. Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond, 2001, MIT Press
[6] Math Works, Statistics and Machine Learning Toolbox, https://jp.mathworks.com/products/statistics.html (参照 2017/08/10)
[7] C.Li, Z.Lu, K.Zhou.. An Image Watermarking Technique Based on Support Vector Regression. IEEE international Symposium on Communications and Information Technology, 2005, Proceedings of ISICT 2005, pp. 183-186
[8] L.Sanping, Z.Yusen, Z.Hui.. A Wavelet-domain Watermarking Technique Based on Support Vector Regression. 2007 International Conference on Grey Systems and Intelligent Services, 2007, pp1112-1116. Nanjing
[9] X.Lv, H.Bian, B.Yu, X.Quan.. Color Image Watermarking Scheme Based on Support Vector Regression. 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing,2009, pp. 144-147.Kyoto
[10] R.Mehta, N.Rajpal, V.P.Vishwakarma.. A Robust and efficient image watermarking scheme based on Lagrangian SVR and lifting wavelet transform. International Journal of Machine Learning Cybernetics, Volume8, Issue2, 2017, pp. 379-395
[11] Ryo Sakuma, Hyunho Kang, Keiichi Iwamura, Isao Echizen.: Digital Watermarking Scheme based on Maachine Learning for the IHC evaluation criteria. In Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2017, Smart Innovation, Systems and Technologies, vol 81
[12] M.Antonini, M.Barlaud, P.Mathieu, I.Daubechies.: Image coding using wavelet transform. In IEEE Transactions on Image Processing, vol. 1, no. 2, 1992, pp. 205-220
[13] Math Works, Wavelet Toolbox, https://jp.mathworks.com/products/wavelet.html (参照 2017/08/10)
[14] F.J.MacWilliams, N.J.A. Sloane.: The theory of error-correcting codes. Elsevier,1977, pp. 257-291
[15] Math Works, Block Coding, https://jp.mathworks.com/help/comm/block-coding.html (参照 2017/08/10)