社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

視覚情報保護を考慮した機械学習のための ランダムサンプリング次元削減法

河村　綾菜† 　飯田　健太† 　貴家　仁志†

† 首都大学東京大学院　システムデザイン研究科　〒 191–0065 東京都日野市旭ヶ丘 6–6
E-mail: †{kawamura-ayana,iida-kenta2}@ed.tmu.ac.jp, ††kiya@tmu.ac.jp

あらまし　本稿では，視覚情報保護を考慮した機械学習のための，ランダムサンプリング次元削減法を提案する．近年，クラウドサービスを利用し，プロバイダーの提供する計算資源を利用する計算形態が急速に普及している．しかし，プロバイダーの信頼性欠如や事故によって，データの不正利用，流出，プライバシー侵害などの問題が危惧されている．また，画像データを機械学習に適用する場合には，そのデータ数の膨大さから，次元削減を行うことが一般的である．本稿では，そのような背景から，プライバシー保護と次元削減を同時に考慮した機械学習法を提案する．提案法では，画像をブロックに分割し，そのブロックをランダムにサンプリングすることで次元削減を行う．これにより，画像の視覚情報保護と，相対的な空間情報の保持が可能となる．また，提案法は実質的な鍵の管理を不要とするといった特徴を持つ．最後に，機械学習の一例としてサポートベクターマシンでの顔認証実験を行い，従来法と同程度の精度を維持できることが確認された．
キーワード　次元削減，機械学習，SVM，プライバシー保護

A Dimensionality Reduction Method with Random Sampling for Privacy-Preserving Machine Learning

Ayana KAWAMURA†, Kenta IIDA†, and Hitoshi KIYA†

† Faculity of System Design, Tokyo Metropolitan University　Asahigaoka 6–6, Hino-shi, Tokyo, 191–0065
E-mail: †{kawamura-ayana,iida-kenta2}@ed.tmu.ac.jp, ††kiya@tmu.ac.jp

Abstract　In this paper, we propose a dimensionality reduction method with random sampling for privacy-preserving machine learning. Recently, cloud computing is spreading in many fields. However, the cloud computing has some serious issues for end users, such as unauthorized use and leak of data, and privacy compromise, due to unreliability of providers and some accidents. In addition, due to a huge amount of data, a dimensionality reduction technique is generally carried out in the case of applying image data to machine learning. Because of such a situation, we consider a machine learning scheme considering both privacy-preserving and dimensionality reduction. In this paper, we propose a novel dimensionality reduction technique that is carried out by dividing an image into blocks and sampling the blocks randomly. The proposed scheme allows us to preserve visual information of images and maintain the relative spatial relation between images. In addition, the proposed scheme has a feature that any secret-key management is not required. Some face recognition experiments are carried out by using a support vector machine algorithm as an example of machine learning algorithms to demonstrate the effectiveness of the proposed method.
Key words　dimensionality reduction, machine learning, SVM, privacy-preserving

1. ま え が き

近年，様々な分野において，機械学習の利用が普及してきている．しかし，機械学習の利用には膨大なデータを必要とし，計算コストが高いといった課題が存在する．そのため，プロバイダーの計算資源を利用するクラウドコンピューティングやエッジコンピューティングが用いられることが多い．しかしクラウドコンピューティングの利用は，プロバイダーの信頼性を

前提にしており，その信頼性の欠如や事故によって，データの不正利用や流失，プライバシーの侵害といった問題の発生が危惧されている [1]．今後のクラウドコンピューティングの普及にとって，データの不正利用や流出，エンドユーザーのプライバシーの問題をいかに解決するかが重要な課題となっている．

これらの問題を解決するために，データを直接公開することなく，暗号化したデータを第三者に渡し計算を依頼する方法が盛んに研究されている．その一つに秘密計算がある [2–14]．秘密計算は，一般にマルチパーティプロトコルや準同型暗号に基づき実行される．しかし，暗号化に伴う計算コストの増大が大きいことに加えて，厳密な鍵の管理が必要であり，適用できる応用が限定される．また，秘密計算とは独立に，ユーザーのプライバシーやデータの秘匿性を考慮した知覚暗号化が研究されている [15–21]．それらの応用として，知覚暗号化を用いた機械学習法が検討されている．さらにこれらの方法を用いると，ある条件の下で，暗号化が機械学習の精度に影響を与えないことが示されている [22–25]．これらは広く普及した多くのアプリケーションソフトウェアを直接利用可能であり，暗号化による計算コストの増加もほぼない．ただし，このような方法では，画像の空間情報を保持することは困難であり，物体検出のような画素の相対的な位置情報を利用する機械学習には応用ができない，また鍵の管理が必要であるといった問題点が解決されていない．

また，画像を用いた機械学習では，データ数の膨大さから入力する特徴ベクトルに対して次元削減を施すことが一般的に行われる [26]．代表的な次元削減法としては，ダウンサンプリング法 [27]，ランダム射影 [28]，主成分分析 [29] などがあげられる．このような従来の次元削減法では，データに含まれるプライバシーの保護や空間情報を保持することは考慮されてこなかった．

以上の問題を解決するために，本稿では，視覚情報保護と次元削減を同時に考慮した機械学習法を提案する．これまで機械学習においてプライバシーの保護と次元削減は独立に扱われてきた．提案法は，画像をブロックに分割し，ブロック単位でランダムにサンプリングすることで，画像の視覚情報保護と空間情報の保持を同時に可能とする次元削減法である．また，次元削減後の画像からは原画像を復元することは困難であり，鍵の管理が不要であるといった利点もある．実験では，機械学習法の一例としてサポートベクターマシンを用いた顔認証実験を行い，従来法と比較して提案法は同程度またはそれ以上の精度が得られることを確認した．

2. 準　　備

2.1 機械学習における次元削減

機械学習では，入力された特徴ベクトルをより高速，正確に分類するために，次元削減が行われる．本稿では，2 つの次元削減法を例にして，議論を展開する．

2.2 次元削減法

2.2.1 ダウンサンプリング法

ダウンサンプリング法 [27] は，図 1 に示すように画像を重複のないブロックに分割し，ブロックの平均値を計算することで，

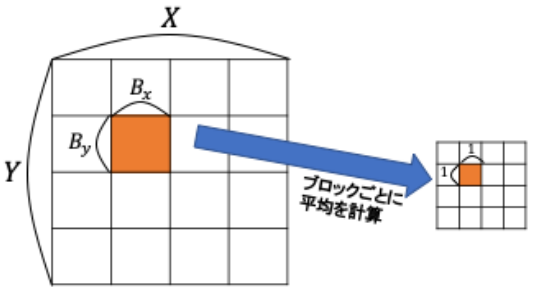


図 1: ダウンサンプリング法

(a) 原画像 (192 × 160)　(b) ダウンサンプリング法 (24 × 20)　(c) ランダム射影 (24 × 20)

図 2: 原画像とその次元削減例

特徴を抽出し次元削減を行う方法である．全てのブロックにおいて同じように平均値を計算することで，次元が $1/(B_x \times B_y)$ に削減された画像を得ることができる．

この方法を用いると，次元を削減する過程でブロック同士の位置関係は変わらないため，画像の相対的な空間情報を保持したまま次元削減することができる．しかし，視覚的な情報は保護することができない (図 2(b) 参照)．

2.2.2 ランダム射影

ランダム射影 [28] は，高次元の特徴ベクトルを低次元の空間に写像することで次元削減を行う方法である．元の d 次元の特徴ベクトル $\boldsymbol{X}, \boldsymbol{Y} \in \mathbb{R}^d$ は以下の式で d_r 次元の空間 ($d_r \leqq d$) に射影される．

$$\boldsymbol{X}^{RP} = \boldsymbol{R}\boldsymbol{X} \tag{1}$$

ここで，$\boldsymbol{X}^{RP}$ は $\boldsymbol{X}$ の射影後の特徴ベクトルであり，$\boldsymbol{R}$ は $d_r \times d$ のランダム行列である．このとき $\boldsymbol{R}$ として $N(0,1)$ の正規分布の乱数を用いることで，高い確率で射影前の特徴ベクトル間のユークリッド距離を保存することが知られている．さらに，$\|\boldsymbol{X}\| \leqq 1$ および $\|\boldsymbol{Y}\| \leqq 1$ を満たすとき，$\boldsymbol{X}$ と $\boldsymbol{Y}$ の間の内積を保存することも示されている．

この方法は，視覚情報を保護することができるが空間情報は保持することができない (図 2(c) 参照)．

3. 提　案　法

上で述べた従来の次元削減法の問題点を解決するために，本稿ではプライバシー保護と空間情報の保持を同時に考慮した次元削減法を提案する．

3.1 プライバシー保護を考慮した認証システム

従来，プライバシー保護を考慮した認証システムでは，図 3 のようなシステムが想定されていた．Client $i, i = 1, ..., N$ は，

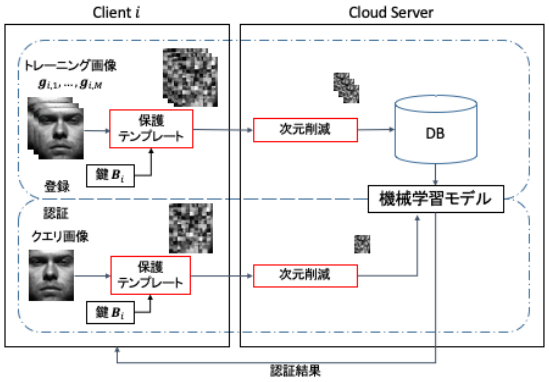


図 3: 認証システム

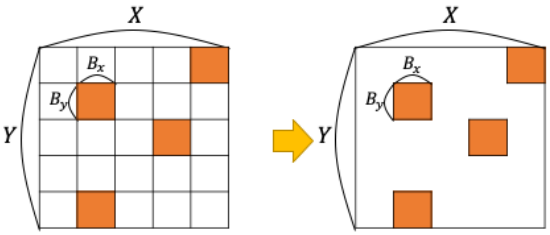


図 4: ブロックのランダムサンプリング

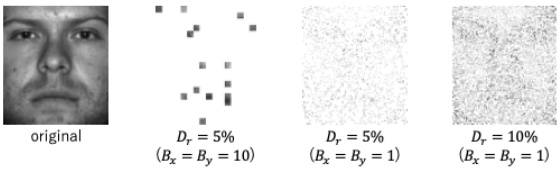


図 5: ランダムサンプリング例

顔画像などのトレーニングデータ $g_{i,j}, j = 1, ..., M$ を準備し，鍵 B_i を用いて M 個の暗号化されたテンプレート (保護テンプレート)$\boldsymbol{I}_{i,j}$ を作成する．次にそれらを Cloud Server に送信する．Cloud Server は，それらに次元削減を施し，データベースに保管すると同時に，機械学習での認証に必要なモデルを保護テンプレートを用いて実行する．認証時には，Client i はクエリから鍵 B_i を用いて保護テンプレートを作成し，Cloud Server へ送信する．Cloud Server は受信した保護テンプレートに次元削減を施し，構築した機械学習モデルを用いて認証を行い，認証結果を Client i に返す．このような認証システムにおいては，画像の視覚情報と鍵はクラウドには与えない．提案法では，以上のシステムにおいて暗号化と次元削減をクライアント側で同時に行う．

3.2 ランダムサンプリング次元削減法

本稿では，画像の次元削減法としてランダムサンプリング次元削減法を提案する．この方法では，画像をブロックに分割し，その中からブロックをランダムにサンプリングすることで次元削減を行う．

提案法の具体的な手順を以下で説明する．まず，$X \times Y$ ピクセルの画像を $B_x \times B_y$ のブロックに分割する．このとき，$B_x \times B_y = 1 \times 1$ とすると，ピクセル単位で次元を削減することに相当する．次に，分割したブロックの中から，鍵によって生成された乱数を用いて図 4 のようにランダムにブロックを選択する．例えば，

$$\text{次元削減率} = \frac{\text{削減後の次元数}}{\text{元の次元数}} \times 100 \qquad (2)$$

が $D_r[\%]$ の場合，選択するブロックの数 n は，

$$n = \frac{X \times Y}{B_x \times B_y} \times \frac{D_r}{100} \qquad (3)$$

で与えられ，n 個のブロックをランダムに選択することによって，次元削減が実行される．元画像の空間情報を保持するために，ブロックの位置の入れ替えは行わない．

図 5 に，ブロックサイズ $B_x = B_y = 1$，次元削減率がそれぞれ $D_r = 5, 10[\%]$ のときの次元削減の例を示す．画像の視覚情報はブロックサイズと次元削減率で制御できることがわかる．機械学習では選択されたブロックの情報を特徴ベクトルとして用いて学習・テストを行う．

3.3 提案法の特徴

提案法の特徴をまとめると，以下のようになる．

(a) 画像の視覚情報を保護できる
(b) 画素の相対的な位置情報を保持できる
(c) 鍵の管理が不要である
(d) 機械学習の高い精度を維持できる

従来法と比較すると，ダウンサンプリング法より (a) の点で，ランダム射影より (b) の点で提案法は従来法よりも優れている．位置情報を保持できることで，物体検出など画像の位置情報を使用する機械学習への応用も期待される．また提案法を用いた場合，クラウドプロバイダーや第三者に鍵が渡ったとしても，次元削減後の画像からは原画像を復元することは困難であり，実質的には鍵の管理が不要となる．さらに後述するように，提案法は従来法と比較して，機械学習において同等またはそれ以上の精度を得ることができる．

4. 実　　験

提案法の有効性を顔認証実験によって評価する．

4.1 実 験 準 備

本実験では，代表的な顔画像データベースである Extended Yale Database B [30] を用いた．38 人の顔画像が 64 枚ずつ，計 2432 枚で構成され，すべて 192 × 160 のサイズに統一されている．各被験者に対する 64 枚の画像を，トレーニング 32 枚とクエリ 32 枚に分けて実験を行った．実験では，機械学習の一例として，サポートベクターマシン (SVM) を用い，RBF カーネルを使用した．RBF カーネルでは，ハイパーパラメータ γ を 81 とした．

また，提案法で使用するブロックサイズは $B_x = B_y = 1, 2, 4, 8$ であり，次元削減率は $1.6, 5, 10, 15, 20[\%]$ の 5 種類を用いた．比較手法としては，従来の次元削減法であるダウンサンプリング法とランダム射影を用い，どちらも次元を 1/64(=1.6[%]) に削減した．図 6 に，原画像とそれぞれの次元削減法によって次元削減された画像を示す．ランダムサンプリング法に使用する

表 1: 従来法との EER の比較 ($D_r = 1.6$[%])

ダウンサンプリング法	ランダム射影	提案法 ($B_x = B_y$)			
		1	2	4	8
0.0443	0.0359	**0.0358**	0.0605	0.1012	0.1304

鍵 B_i は $B_1 = B_2 = ... = B_i$ である．ただし，鍵の管理は実質的に不要である．それぞれの条件において，鍵を変えて 10 回ずつ実験を行った．

(a) 原画像 (192 × 160)　(b) ダウンサンプリング法

(c) ランダム射影　(d) 提案法

図 6: 実験画像とその次元削減例 ($D_r = 1.6$[%])

4.2 実験結果

SVM による顔認識では，DB の各登録者に対して 1 つの分類器が作成される．分類器は，各クエリテンプレートに対する予測ラベルおよび分類スコアを出力する．分類スコアは，クエリから分類境界までの距離である．クエリテンプレートの正のラベルに対する分類スコア S_q と閾値 τ との間の関係は以下のように与えられる．

$$if\ S_q \leqq \tau\ then\ accept;\ else\ reject. \qquad (4)$$

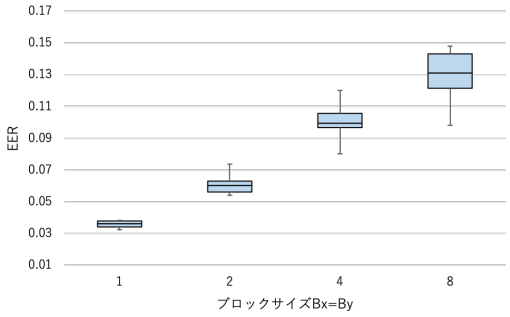
実験での評価尺度には，本人棄却率 (False Reject Rate : FRR) と他人受理率 (False Accept Rate : FAR)，それらが等しくなる点である等価エラー率 (Equal Error Rate : EER) を用いた．

提案法を用いて実験を行ったときの EER を図 7 に示す．これより，ブロックサイズ $B_x = B_y$ が小さいほど，また次元削減率 D_r が大きいほど EER が向上する．

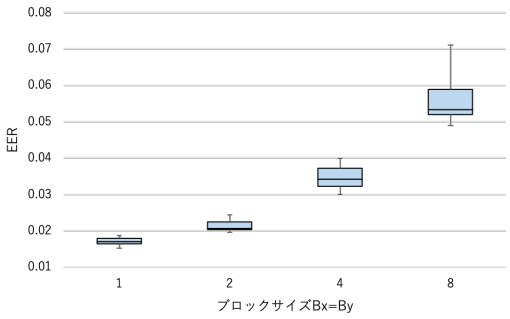
ダウンサンプリング法，ランダム射影，提案法の EER を次元削減率 1.6[%] で比較したものを表 1 に示す．ここで，ランダム射影と提案法の結果は 10 回実験を行ったときの EER の平均値である．表 1 より，提案法は $B_x = B_y = 1$ のとき従来法よりも EER が向上していることがわかる．従って，提案法は画像の視覚情報保護と空間情報の保持が可能となるだけでなく，従来法と同程度以上の精度を維持できることが確認された．

5. まとめ

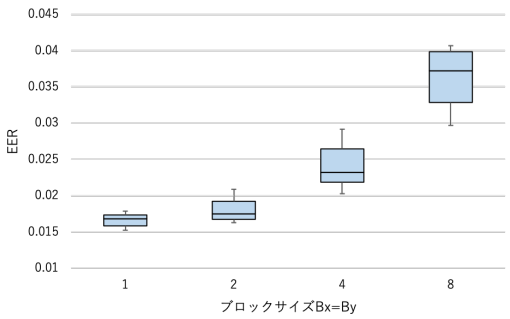
本稿では，視覚情報保護を考慮した機械学習のためのランダムサンプリング次元削減法を提案した．提案法では，視覚情報を保護し，かつ空間情報を保持した特徴ベクトルの生成を可能とした．実験では，提案法は，画素単位のランダムサンプリングを用いることで，上記の特徴に加え，従来のランダム射影やダウンサンプリング法といった次元削減法と比較して，機械学習の精度を低下させないことが確認された．今後は，画像の空間情報を使用する機械学習への応用を検討している．



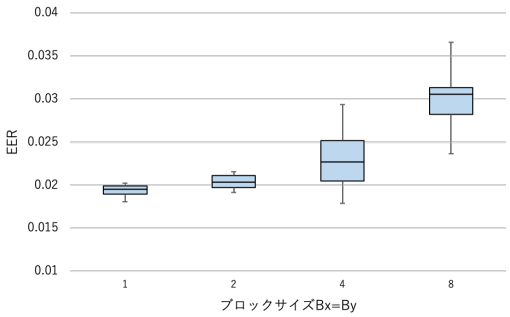
(a) D_r=1.6[%]



(b) D_r=5[%]



(c) D_r=10[%]



(d) D_r=20[%]

図 7: 提案法の EER

謝辞

本研究の一部は，首都大学東京傾斜的研究費 (全学分) 学長裁量枠戦略的研究プロジェクト戦略的研究支援枠「ソーシャ

ルビッグデータの分析・応用のための学術基盤の研究」，及び JSPS 科研費 JP17H03267(基盤研究 (B) 一般)「プライバシー保護のための画像圧縮を可能とする知覚暗号化とその攻撃耐性」の助成を受けたものである．

文　献

[1] C.T. Huang, L. Huang, Z. Qin, H. Yuan, L. Zhou, V. Varadharajan, and C.C.J. Kuo, “Survey on securing data storage in the cloud,” APSIPA Transactions on Signal and Information Processing, vol.3, no.e7, 2014.

[2] R. Lazzeretti and M. Barni, “Private computing with garbled circuits [applications corner],” IEEE Signal Processing Magazine, vol.30, no.2, pp.123–127, 2013.

[3] M. Barni, G. Droandi, and R. Lazzeretti, “Privacy protection in biometric-based recognition systems: A marriage between cryptography and signal processing,” IEEE Signal Processing Magazine, vol.32, no.5, pp.66–67, 2015.

[4] R. Lagendijk, Z. Erkin, and M. Barni, “Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation,” IEEE Signal Processing Magazine, vol.30, no.1, pp.82–105, 2013.

[5] T. Araki, A. Barak, J. Furukawa, T. Lichter, Y. Lindell, A. Nof, K. Ohara, A. Watzman, and O. Weinstein, “Optimized honest-majority mpc for malicious adversaries - breaking the 1 billion-gate per second barrier,” IEEE Symposium on Security and Privacy (SP), pp.843–862, 2017.

[6] Y. Aono, T. Hayashi, L. Phong, and L. Wang, “Privacy-preserving logistic regression with distributed data sources via homomorphic encryption,” IEICE Transactions on Information and Systems, vol.E99.D, no.8, pp.2079–2089, 2016.

[7] R. Shokri and V. Shmatikov, “Privacy-preserving deep learning,” Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp.1310–1321, 2015.

[8] L. Phong, Y. Aono, T. Hayashi, L. Wang, and S. Moriai, “Privacy-preserving deep learning via additively homomorphic encryption,” IEEE Transactions on Information Forensics and Security, vol.13, no.5, pp.1333–1345, 2018.

[9] L.T. Phong and T.T. Phong, “Privacy-preserving deep learning for any activation function,” CoRR, vol.abs/1809.03272, 2018.

[10] N. Dowlin, R. Giladbachrach, K. Laine, K. Lauter, M. Naehrig, and J. Wemsing, “Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy,” MSR-TR-2016-3, Microsoft TechReport, 2016.

[11] Y. Wang, J. Lin, and Z. Wang, “An efficient convolution core architecture for privacy-preserving deep learning,” Proc. IEEE International Symposium on Circuits and System, 2018.

[12] H. Yang, Y. Huang, Y. Yu, M. Yao, and X. Zhang, “Privacy-preserving extraction of hog features based on integer vector homomorphic encryption,” International Conference on Information Security Practice and Experience, pp.102–117, 2017.

[13] Q. Wang, J. Wang, S. Hun, Q. Zou, and K. Ren, “Sechog: Privacy-preserving outsourcing computation of histogram of oriented gradients in the cloud,” Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, pp.257–268, 2016.

[14] A.M. Saxe, Y. Bansal, J. Dapello, M. Advani, A. Kolchinsky, B.D. Tracey, and D.D. Cox, “On the information bottleneck theory of deep learning,” International Conference on Learning Representations, 2018.

[15] I. Nakamura, Y. Tonomura, and H. Kiya, “Unitary transform-based template protection and its properties,” Proc. European Signal Processing Conference, vol.SIPA-P3.4, pp.2466–2470, 2015.

[16] I. Nakamura, Y. Tonomura, and H. Kiya, “Unitary transform-based template protection and its application to l2-norm minimization problems,” IEICE Trans. Inf. Sys, vol.E99-D, no.1, pp.60–68, 2016.

[17] T. Chuman, W. Sirichotedumrong, and H. Kiya, “Encryption-then-compression systems using grayscale-based image encryption for jpeg images,” IEEE Transactions on Information Forensics and security, vol.14, no.6, pp.1515–1525, 2019.

[18] W. Sirichotedumrong and H. Kiya, “Grayscale-based block scrambling image encryption using ycbcr color space for encryption-then-compression systems,” APSIPA Transacrions on Signal and Information Processing, vol.8, e7, 2019.

[19] K. Kurihara, S. Shiota, and H. Kiya, “An encryption-then-compression system for jpeg standard,” Picture Coding Symposium (PCS), pp.119–123, 2015.

[20] K. Kurihara, M. Kikuchi, S. Imaizumi, S. Shiota, and H. Kiya, “An encryption-then-compression system for jpeg/motion jpeg standard,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.98, no.11, pp.2238–2245, 2015.

[21] K. Kurihara, S. Imaizumi, S. Shiota, and H. Kiya, “An encryption-then-compression system for lossless image compression standards,” IEICE transactions on information and systems, vol.E100-D, no.1, pp.52–56, 2017.

[22] 前川貴大, 木下裕磨, 塩田さやか, 貴家仁志, “ランダムユニタリ変換を用いたプライバシー保護を考慮した SVM 学習法,” 電子情報通信学会 画像工学研究会, vol.117, no.200, pp.13–18, 2017.

[23] 河村綾菜, 前川貴大, 木下裕磨, 貴家仁志, “EtC 画像を用いた暗号化領域での SVM 学習法,” 電子情報通信学会スマートインフォメディアシステム研究会, vol.118, no.73, pp.1–6, 2018.

[24] 河村綾菜, 前川貴大, 木下裕磨, 貴家仁志, “次元削減を考慮した暗号化領域での SVM 学習法,” 電子情報通信学会マルチメディア情報ハイディング・エンリッチメント研究会, vol.118, no.224, pp.7–12, 2018.

[25] T. Maekawa, A. Kawamura, Y. Kinoshita, and H. Kiya, “Privacy-preserving support vector machine computing using random unitary transformation,” IEICE Trans. Fundamentals, vol.E102-A, no.12, 2019, (to be published).

[26] P.T. Boufounos, H. Mansour, S. Rane, and A. Vetro, “Dimensionality reduction of visual features for efficient retrieval and classification,” APSIPA Transactions on Signal and Information Processing, vol.5, 2016.

[27] J. Wright, A. Yang, A. Ganesh, S. Sastry, and Y. Ma, “Robust face recognition via sparse representation,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol.31, no.2, pp.210–227, 2009.

[28] E. Bingham and H. Mannila, “Random projection in dimensionality reduction: applications to image and text data,” Proceedings of the seventh ACM SIGKDD International Conference on Knowledge Discovery and Dara Mining, 2001.

[29] S. Wold, K. Esbensen, and P. Geladi, “Principal component analysis,” Chemometrics and Intelligent Laboratory Systems, vol.2, pp.37–52, 1987.

[30] A. Georghiades, P. Belhumeur, and D. Kriegman, “From few to many: Illumination cone models for face recognition under variable lighting and pose,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol.23, no.6, pp.643–660, 2001.