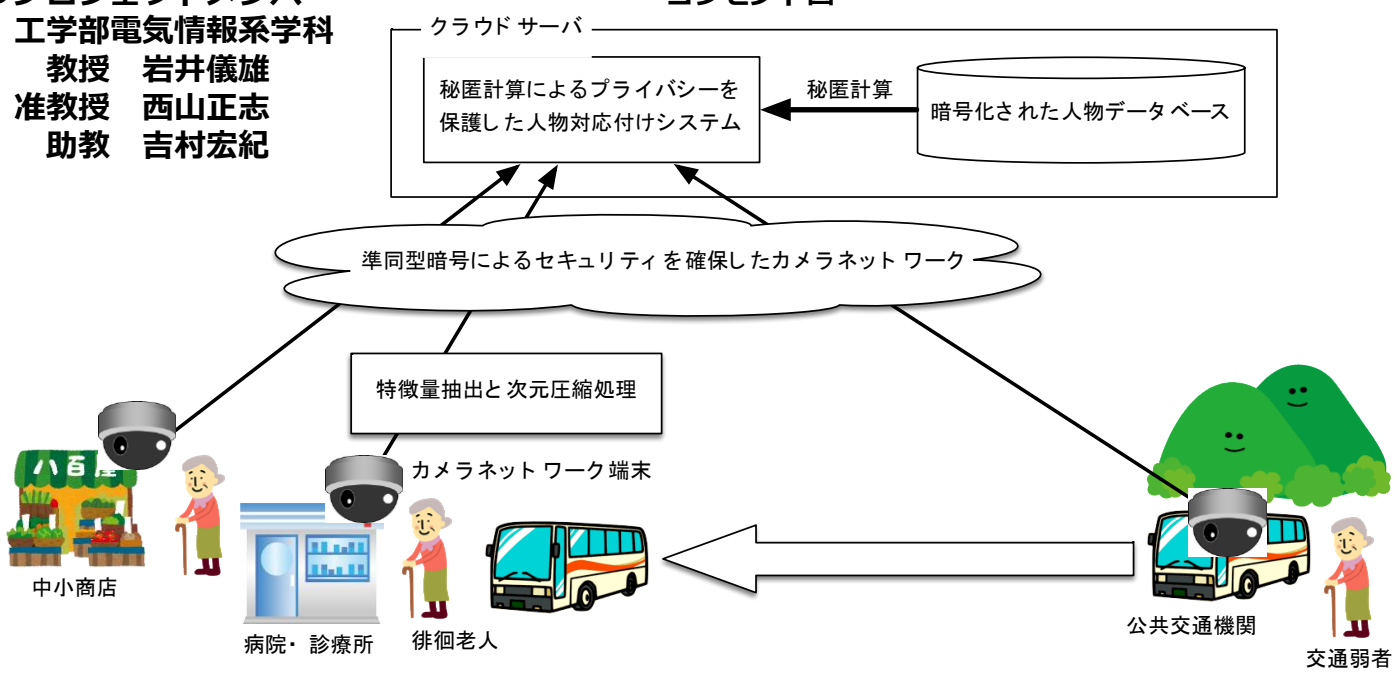
準同型暗号を利用した
人物対応付け手法の研究開発

●プロジェクトメンバー
工学部電気情報系学科
教授　岩井儀雄
准教授　西山正志
助教　吉村宏紀

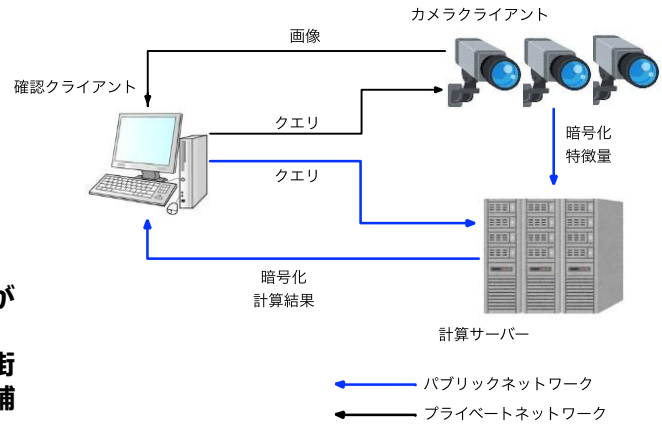
コンセプト図



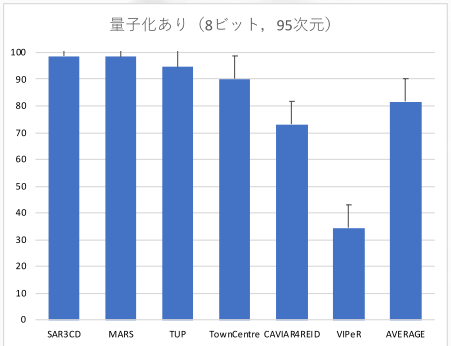
研究概要:

・カメラネットワーク端末で撮像された人物画像を暗号化してクラウドサーバに伝送し、暗号を復号せずにそのままプライバシーを保護した状態でカメラ間での人物対応付けを行う手法の研究開発をいます。

実用化できれば、いつでも何処でも人物を対応付けることができ様々な人物画像認識システムを構築することが可能となります。応用として、人物同定による社会の安全性向上（防犯目的）、高齢者や子供のみ守り、商店街のカメラを用いた人物流解析，動線解析による都市や店舗のレイアウト計画など多種多様なものに展開可能です。



システム概略図



各データベースの対応付け精度

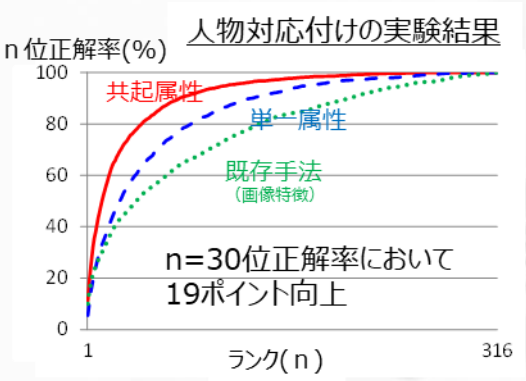
防犯カメラで撮像される映像はプライバシーの問題があり、クラウドサーバ上での画像データの漏えい、個人が特定され行動が監視されるのではないか問題となっています。そのため、クラウドサーバ上においても、暗号化人物データを復号せずに、暗号のまま対応付けなどの処理を行う秘匿計算が必要です。そこで、準同型暗号に着目し、プライバシーを保護した人物対応付けの秘匿計算に適した手法を研究開発しています。
本研究は、総務省のSCOPEや科研費基盤(C)等に採択されており、学会においても、Student Paper Award や優秀学術賞を受賞しており、本研究は高く評価されています。

(1) Morita, K., Yoshimura, H., Nishiyama, M., Iwai, Y., Protecting Personal Information using Homomorphic Encryption for Person Reidentification, Proc. IEEE 7th Global Conf. on Consumer Electronics, pp. 135-136, 2018. (Student Paper Award)

研究開発の内容及び成果：

防犯カメラに映った人物の見え方は，撮影されたときの姿勢・照明・距離の変化により様々に変化します。我々の開発した共起属性により、様々に変化する人物画像を頑健に高い精度で認識できるようになりました。複数のデータベースを用いて評価し、平均10位正解率で90%以上を達成しました。さらに準同型暗号を組み込むことで個人情報を保護できる仕組みを構築しました。また、この仕組みを用いてクラウドサーバシステムを構築して、システムの運用可能性を検証し、1件当りの処理時間 0.2秒のスループットを得ました。

人物対応付けシステムの概念図



今後の研究開発成果の展開および波及効果創出への試み：

本研究開発では，準同型暗号を利用した人物対応付けの手法を研究開発し、高い認識性能を達成することが出来たが、一方で準同型暗号がもたらす大量のデータのために、一般的なクラウドサービスに利用できるほどにはデータの圧縮効率は高くない。また，鳥取県のような過疎地域におけるシステムとして個人事業者がクラウドサーバを維持できるというのも難しいという現状がある。そのため、クラウドサービスの研究開発を引き続き進める予定である．また、さらなる競争的資金に応募し、クラウドサーバを試験的に立ち上げることで人物対応付けサービスの可能性の検討を行う予定である．

(2) 山口 紗也加, 吉村 宏紀, 西山 正志, 岩井 儀雄, 視線位置分布を用いたランダムフォレスト改良による人物性別の認識, 画像センシングシンポジウム (SSII), IS3-28, pp. 1-5, June 2018.（優秀学術賞）
(3) 福田 尚悟, 森田 一成, 吉村 宏紀, 西山 正志, 岩井 儀雄, 人物対応付けにおける姿勢と照明に頑健な画像選択手法の検討, IEEE広島支部学生シンポジウム (HISS), pp. 273 - 276, Nov. 2018.（優秀研究賞）
(4) 井上 路子, 西山 正志, 岩井 儀雄, プライバシーが保護された訓練画像に対する視線位置分布を用いた性別認識, 精密工学会誌, vol.85 , no.12, pp. 1094 - 1101, December 2019.