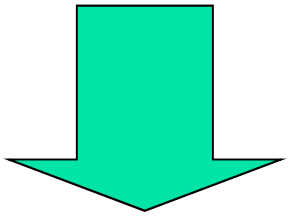
信頼されていないコンピュータ環境での安全な指紋認証システム

渡邊研究室　五島秀典

背景

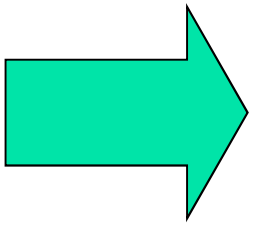
情報システム、ビルシステムの保護
する必要がある。



暗証番号、ICカードなどアクセスするため
設備の設置を行う。

欠点

- 盗難
- 紛失



- パスワード、ICカードなしでは本人でも認証不可
- パスワード、ICカードがあれば他人でも認証可能

重大な欠点

近年の傾向

- 生体認証の実装

  静脈認証、指紋認証、虹彩認証　etc

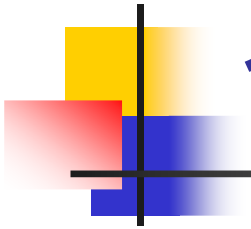
- 利用場所

  家のカギ、金庫へのアクセス　　etc

- 将来の利用

  電子取引システム、リモートアクセスの個人認証　　etc

  さまざまなシステムの遠隔認証システム

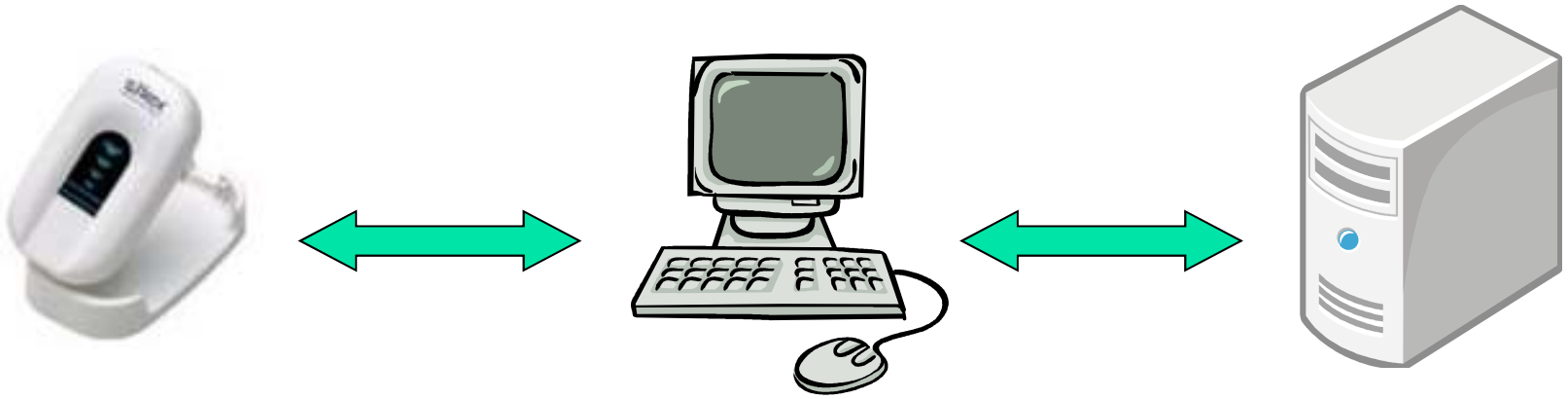


今後の必要性

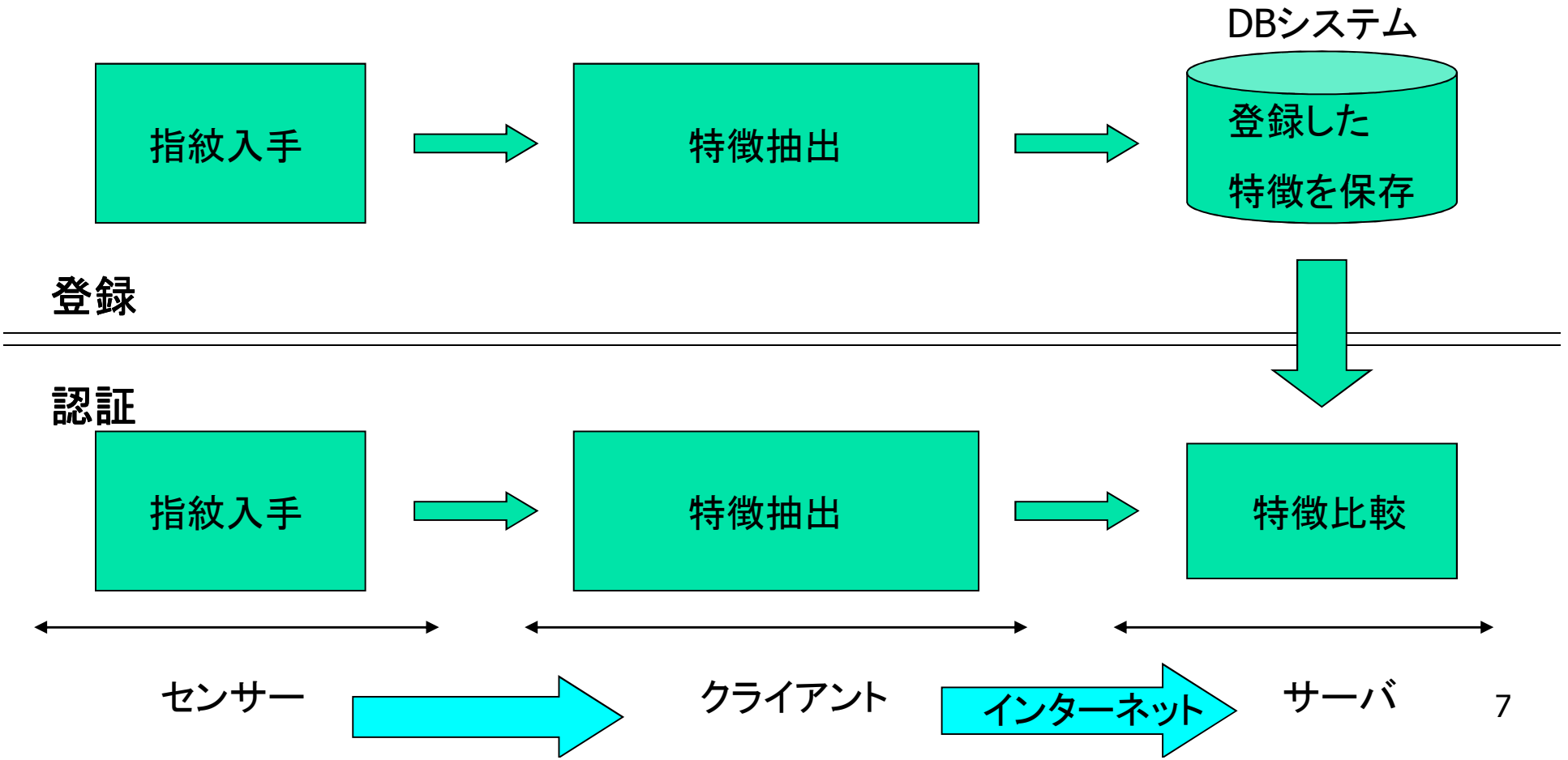
- 信頼できないクライアントがいても安全性が保障される
- 利用者増大に対応できるようにするためにスケーラブルなシステム

提案する方式に使用するモデル

- 生体認証の指紋認証システムについて
- センサ・クライアント・サーバモデルを使用



指紋認証システム


DBシステム
指紋入手
特徴抽出
登録した
特徴を保存
登録
認証
指紋入手
特徴抽出
特徴比較
センサー
クライアント
インターネット
サーバ

システムへの攻撃

- 通信チャンネルへの攻撃
- モジュールへの攻撃
- トロイの木馬 
- 反射攻撃 (リプレイアタック)　　など

トロイの木馬

- コンピュータ上のソフトウェア。

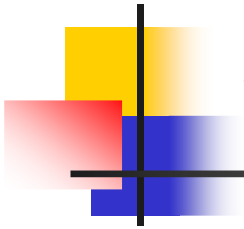
安全だと思うようなソフトウェアになり済まして悪事を働く。

- 動作

実行することでサーバとなる

サーバとなったpcにクライアントを使用することで好きな時に被害者のpcに接続可能

指紋認証システムでは前回認証したデータを使用し、不正にアクセス、正規ユーザの認証阻止



提案方式①

- 目指すシステム

  スケーラブルであるシステム

  クライアントへのトロイの木馬攻撃に対して安全なシステム

  (サーバに対しては専門家によって守られているため)

- 前提条件

  使用するセンサとして最低限のプロセッサを持っていること

提案方式②

- 特徴抽出をサーバではなくセンサ、クライアントに割り当てる

理由

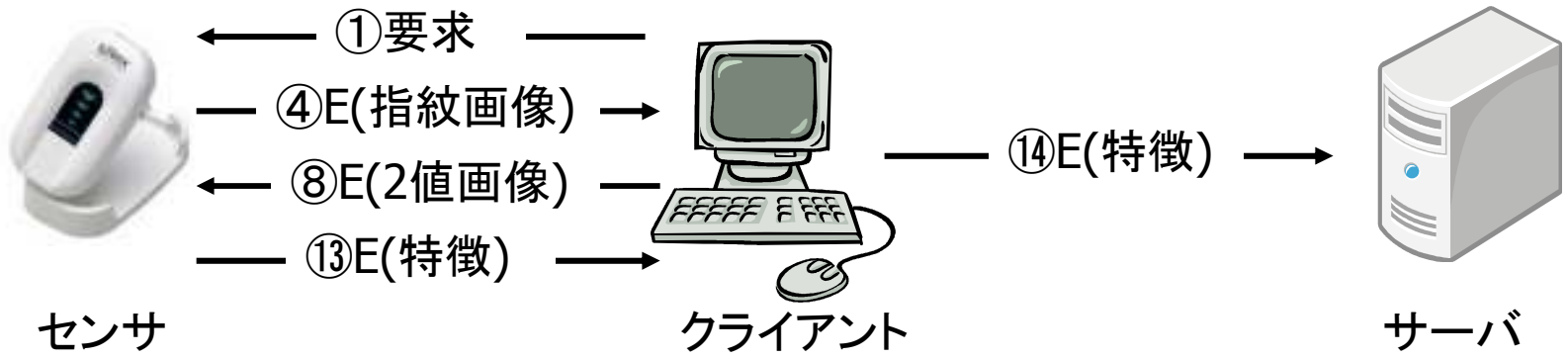
特徴抽出はこのシステムで1番コンピュータに負荷をかけるためサーバに割り当ててしまうとスケーラブル性を達成できなくなるため。

- 特徴抽出を2値化と2値画像からの特徴抽出に分ける

理由

特徴抽出の中でも2値化は計算がたくさん必要でセンサでは時間がかかるため、2値化画像からの特徴抽出をセンサに割り当て、2値化をクライアントに割り当てている。

提案方式(動作)



②指紋獲得と確認画像生成

③指紋暗号化

⑨2値画像復号

⑩2値画像のチェック

⑪2値画像から特徴抽出

⑫特徴を暗号化

⑤指紋を復号

⑥2値画像生成

⑦2値画像暗号化

⑮特徴を復号

⑯特徴比較

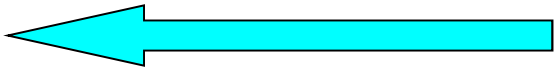
※⑬,⑭の時にクライアントを通っているがサーバとセンサの間で共通するカギで暗号化しているためクライアントは内容の変更ができなくなっている。

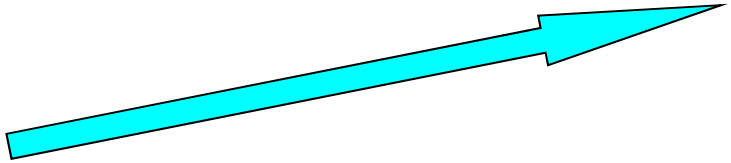
センサでの2値画像のチェック

センサ

指紋画像を取得と同時に確認イメージを生成

左：確認画像　右：取得画像





クライアント

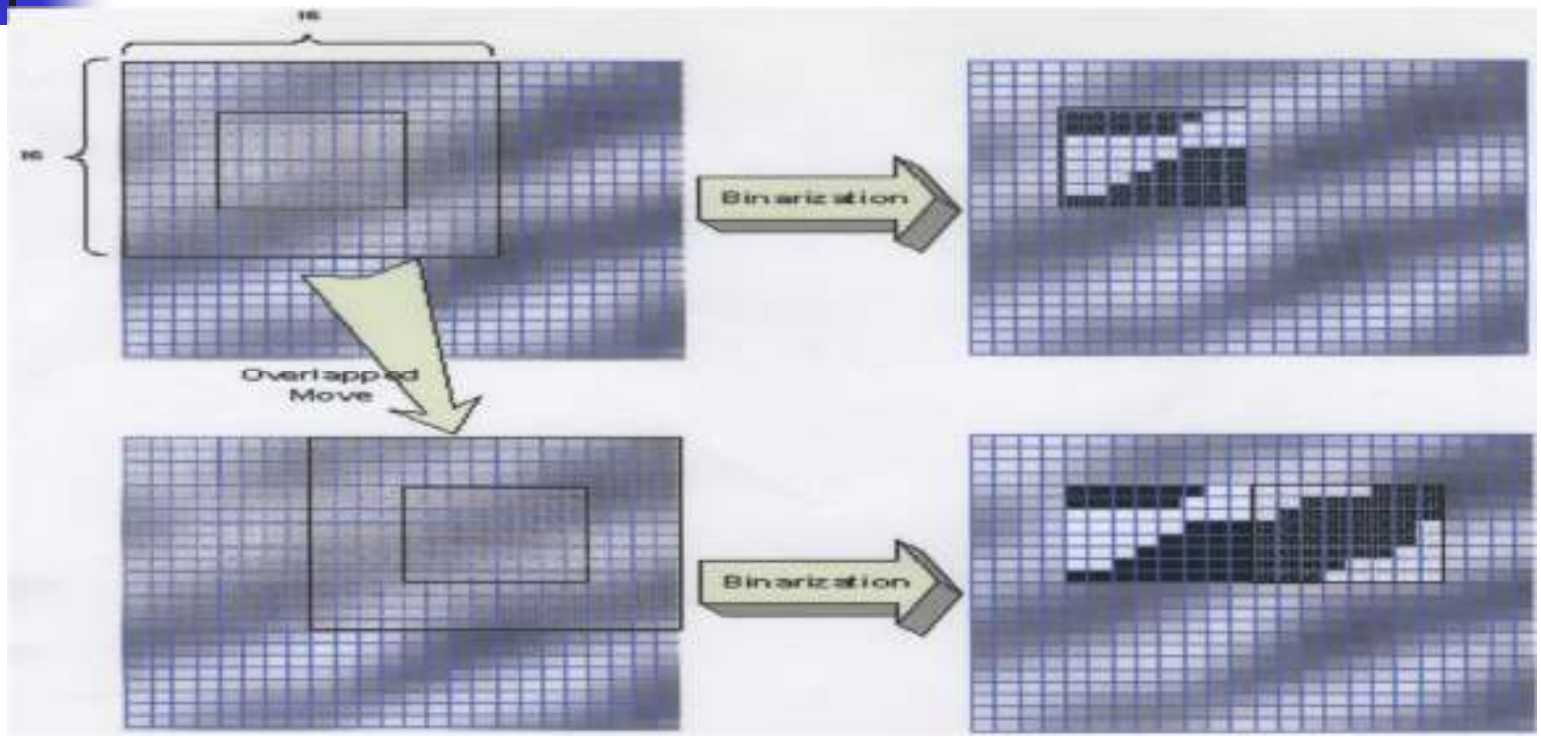
普通はもらった画像を2値化するが、トロイの木馬によって違う画像にすり替え、センサに送信するかもしれない・・・・

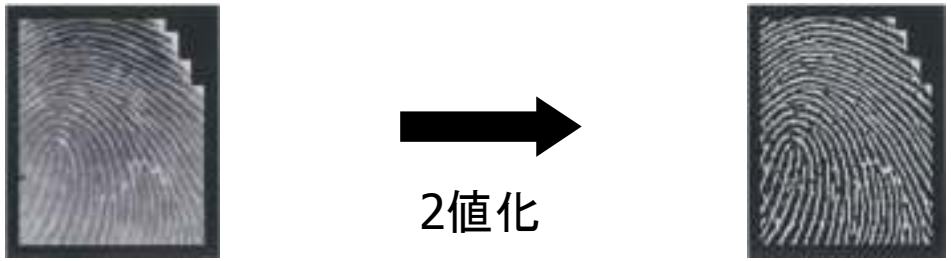
信頼できないクライアントが返した2値画像が先ほど取得した指紋画像から作られた2値画像かを確認イメージを用いてリアルタイムでチェックする

簡単な2値化アルゴリズム

取得した画像　　スムージング後の画像　　背景と指紋画像の分割後の画像　　2値化後の画像

簡単な2値化アルゴリズム





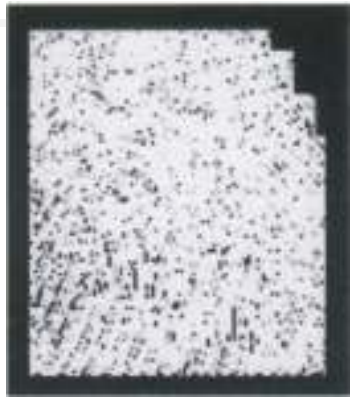
性能評価

取得画像

クライアントから得られた画像(同じ場合)

クライアントから得られた画像(違う場合)

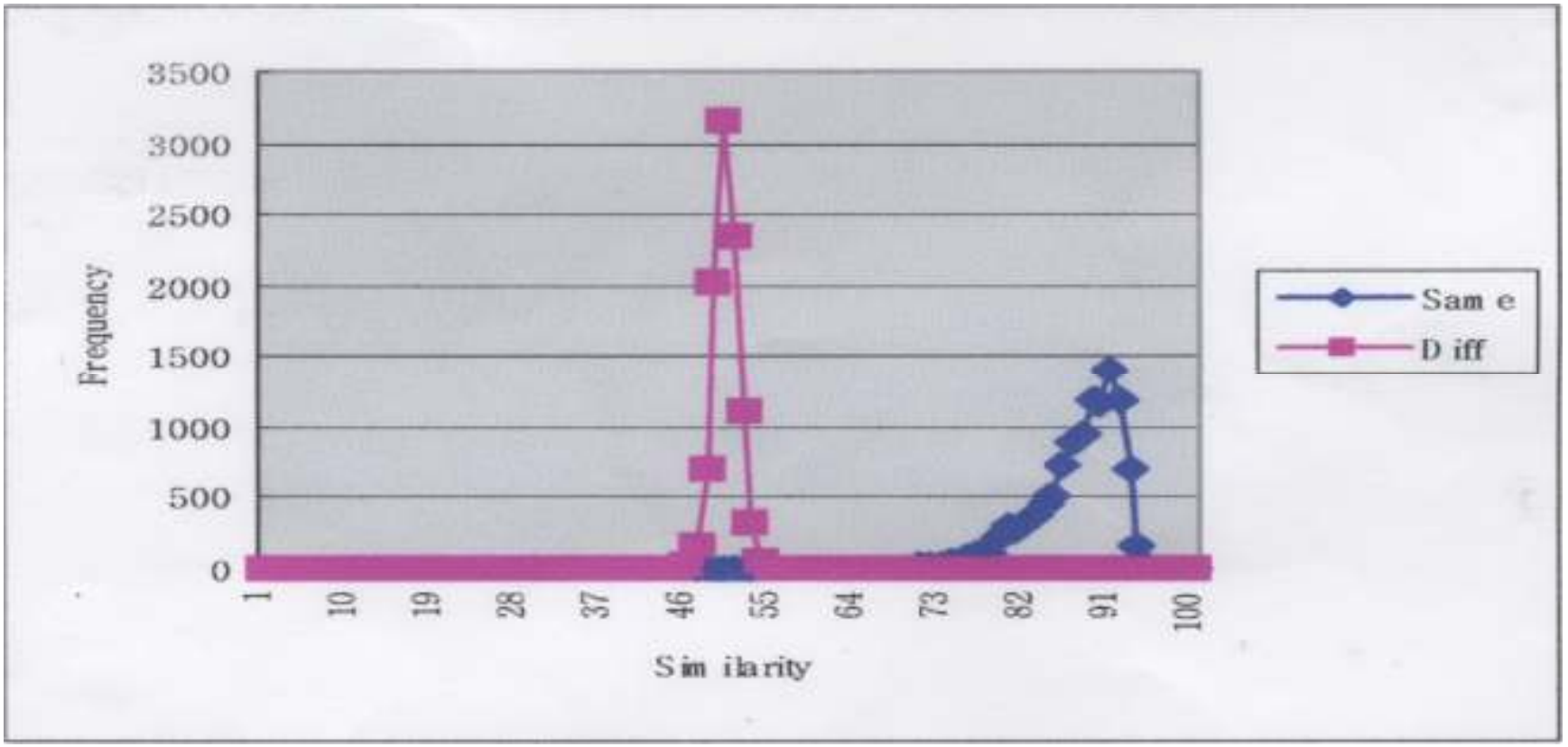
センサから得られた確認イメージ

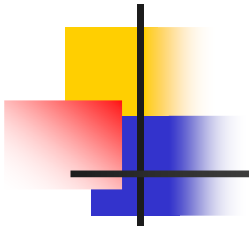


同じ時の画像を重ね合わせた結果

違う時の画像を重ね合わせた結果

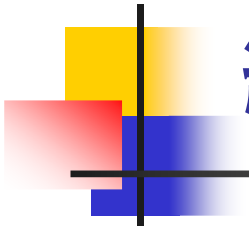
類似性に関するグラフ


3500
3000
2500
2000
1500
1000
500
0
Frequency
1
10
19
28
37
46
55
64
73
82
91
100
Similarity
Same
Diff



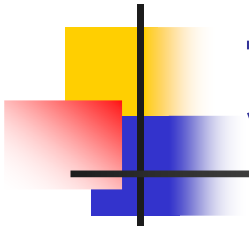
2値化の速度

	ペンティアム4CPU (2GHz)	ARM7CPU (28.5Mhz)
典型的なアルゴリズム	0.74 秒	6.5秒
提案するアルゴリズム	0.0341秒	0.265秒



結論

- 実験結果に基づいて、スケーラブル、および信頼されていないクライアントの援助によるリアルタイムに確認することでトロイの木馬からも安全なセンサクライアント・サーバモデルに指紋照合の提案方法が有効である。



文献

論文

A Secure Fingerprint Authentication System on an Untrusted Computing Environment

著者

Yongwha Chung, Daesung Moon, Taehae Kim and SungBum Pan

作成年

2005年