それから彼らは彼を連れて行き、ヨルダンの通路で彼を殺した。その時、エフライミテスは四十二千人落ちた。  
1はじめに上記の引用は、認証が人間の特性に依存するセキュリティプロトコルの最初の記録された軍事利用である可能性があります。この場合、彼のアクセントです。  
）バイオメトリクスは、個々の解剖学の生理機能の一部の側面（手の形状や指紋など）、深く根付いたスキルや動作（手書きの署名など​​）、またはこれら2つの組み合わせ（音声など）を測定することで人々を識別します。  
1。  
 海外への旅行は、国際標準の生体認証旅行書類、米国への訪問者を指揮するUS-VISITプログラム、および欧州連合の国境にある顔認識パスポートブースによってスピードアップされました。  
2。  
 2012年以降、ディープニューラルネットワークの革命によってもたらされた顔認識技術に大幅な改善がありました。  
3。  
 人々は自分の人生を自分の電話、または自分の電話が資格情報を持っているWebサービスで維持しているので、紛失または盗難に遭った電話を煩わしさから災害に変えるのに頼っています。  
2005年には50億ドル[997]、2019年には330億ドル[2038]。  
17。  
 ヨーロッパはその逆だった。中世にはアザラシが使用されたが、ルネサンスの人々が文書に同意するために自分の名前を書くようになった後、書面が広まった。  
 毎日、数十億ドル相当の契約が手書きの署名によって結ばれています。これらが電子メカニズムによってどのように置き換えられるかは、現在の政策と技術の問題のままです。  
 重要な要素は、偽造の責任です。  
 これらの国では、銀行がほとんどのリスクを負うため、原稿の署名は顧客にとってより優れていますが、PINと電子トークンは銀行にとってより優れている可能性があります。  
米国では、法律により銀行が電子システムを導入する責任を負うため、米国の銀行は通常、チップとPINを使用するのではなく、チップと署名カードを使用しています。  
 したがって、手書きの署名の検証は引き続き重要です。  
 店舗での多くの銀行カード取引は、標本を一目見なくても受け入れられます。セキュリティエンジニアリング523ロスアンダーソン17。  
 手書きの署名カードの署名–多くのアメリカ人は自分のクレジットカードに署名する必要さえありません。  
 実験では、それぞれ144のペアワイズ比較を行った105人の専門文書審査官が、6つの誤解を招いたことが示されました。  
一方、同じ教育レベルの訓練を受けていない34人のコントロールグループは、38人を間違えました。  
 専門家による誤りは業界で継続的な議論の対象となっていますが、審査官の先入観[198]と文脈[587]を反映するように考えられています。  
ほとんどの英語圏では、ほとんどのドキュメントは特別な手段による認証を受ける必要はありません。  
 したがって、電子メールメッセージの下部にあるプレーンテキスト名には、反対の特別な規制がある場合を除き、完全な法的効力があります[2042]。  
 たとえば、あなたが定評のある顧客ではない銀行から借り入れたお金を使ってイングランドの家を購入するには、パスポートなどの書類を持って弁護士事務所に行き、所有権に署名します契約を譲渡および貸与し、弁護士に連署させます。  
他のタイプの文書（専門家の証言など）は、特定の方法で非公証する必要がある場合があります。  
 一部の国では、機械書面による契約を各ページで開始する必要がありますが、そうでない場合もあります。慣習の衝突は依然として深刻な問題を引き起こします。  
 したがって、この弱い生体認証メカニズムは実際にはかなり適切に機能します。実際の問題は、国やアプリケーションによって異なる手続き規則の茂みから生じます。  
セクション26。  
2私は、Webページのボタンをクリックして行われた契約を合法化した2000年のGlobal and NationalCommerce（「ESIGN」）法の電子署名と、すべての加盟国が電子署名を受け入れることを要求するはるかに重いヨーロッパのeIDASRegulation（910/2014）について説明します承認された製品を使用して作られました。カードに署名することは銀行の利益ではありますが、顧客の利益ではありません。  
2。  
 署名サービスは通常、トップレットが手書きであると想定される、機械で作成された署名付きの電子ドキュメントを生成します。また、信頼できるサービスプロバイダーによる検証が必要な電子署名もあります。  
 これは、銀行に小切手処理装置を販売する企業によって、1980年代に本格的な生体認証研究の初期のトピックの1つになりました。  
 コスト上の理由から、これは数千ドルを超える金額に対してのみ行われました。小さな小切手は真っ直ぐ通り抜け、異議を唱えるのはアカウント所有者の責任でした。  
 これらは、配達ドライバーが商品のレシートを収集するために使用し、クレジットカード取引にも使用されます。  
アラームと同様に、ほとんどの生体認証システムは、銀行業界では詐欺および侮辱率と呼ばれ、生体認証の文献ではタイプ1およびタイプ2のエラーと呼ばれています。  
 トレードオフは受信機の動作特性として知られており、レーダー運用者が最初に使用した用語です。レーダーセットのゲインを上げすぎるとターゲットのクラッターが見えなくなりますが、小さすぎるとまったく見えなくなります。  
 等しいエラー率とは、システムが調整されて、偽の受け入れと偽の拒否の確率が等しくなる場合です。  
 自動比較は、人間の精査のためのチェックを選択するためのフィルターとして使用されるため、チェック処理センターなどの操作では致命的ではありません。  
百のトランザクションの1つが失敗した場合、顧客への悪化は受け入れられないでしょう。  
01％。これは、署名検証と指紋スキャンでの最新技術を超えていました。実際、まだ[719]です。  
ベンダーは通常、アイリススキャナーと指先が摩耗した肉体労働者の統計から、目の見えない人を指紋の統計から除外します。  
一般に、生体認証メカニズムは、警備員を置き換えるのではなく、警備員を支援する有人運用でより堅牢になる傾向があります。  
3。  
3顔認識顔の特徴で人を認識することは、少なくとも私たちの初期の霊長類の祖先にさかのぼって、すべての最も古い識別メカニズムです。  
 たとえば、他の人が私たちを見ているかどうかを検出することは非常に得意です。  
 運転免許証、パスポート、その他の種類のIDカードは、コンピューター室への入室を直接制御するためだけでなく、他のほとんどのシステムのブートストラップにも使用されます。  
では、フレッシュで友達を識別するのとは対照的に、写真付きIDで見知らぬ人を識別するのはどれほど優れているのでしょうか？  
 彼らは44人の学生を募集し、それぞれに異なる写真が書かれた4枚のクレジットカードをそれぞれに発行しました。•写真の1つは「良い、良い」写真でした。  
 それは本物でしたが少し古く、学生は今や異なる服や髪型などを持っています。  
 さまざまな人々のランダム写真100枚ほどの山の中から、調査員は主題のように見えるものを選びました。  
 被験者と同じ性別と人種であったことを除いて、無作為に選択されました。  
実験は通常の営業時間後にスーパーで行われたが、経験豊富なレジ係が勤務し、実験の目的を認識していた。  
チェックアウトステーションのどれもが「良い、悪い」写真と「悪い、良い」写真の違いを見分けることができないことが判明しました。  
 現在、この実験は最適な条件下で行われ、経験豊富な待機時間、十分な時間、カードが拒否された場合の恥ずかしさや暴力の脅威はありません。  
 実際、多くのストアは、クレジットカード会社が盗んだカードを手に入れたことに対する報酬をチェックアウトステーションに渡しません。  
 それでも、クレジットカードの写真で実験を行った少なくとも2つの銀行では、かなりのセキュリティエンジニアリング526ロスアンダーソン17が発生しました。  
 顔認識詐欺の減少[154]。  
したがって、人々が身元確認のコンテキストで顔認識スキルを効果的に使用しない場合や、ソーシャルコンテキストで人々を識別するために使用する情報が、1枚の写真を見たときに得られる情報とは異なる方法で脳に保存される場合があります。  
 誤認は偽装監獄の主な原因であると考えられており、目撃者の20％はアイデンティティパレードで間違いを犯しています[2044]-顔と写真を比較したときのほぼランダムな結果ほど悪くはありませんが、それでもまだ良くはありません。試みは19世紀にさかのぼります。当時、フランシスガルトンは、顔面の測定用に一連のばね式「機械式セレクター」を考案していました[738]。  
 自動化されたパスポートコントロールブースが最も簡単な場合があります。被写体は、制御された照明条件の下でカメラをまっすぐ見て、ファイルに写っている顔と比較されます。  
 最も難しいのは監視です。そこでは、空港で動いている人々の群れをスキャンして、数千人の既知の容疑者のリストに載っている人をピックアップしようとします。  
 1998年、ロンドンのニューハム自治区は目立つ通りにビデオカメラを設置し、彼らの新しいコンピューターシステムが群衆の中で顔をスキャンして数百人の知られているローカル犯罪者を絶えずスキャンする方法についてPRキャンペーンを行いました。  
 9/11以降、多くの場所でこれが試されました。  
 ボストンのローガン空港でも顔認識が試みられました。保安検査を通過する乗客が観察され、一致した。  
 イリノイ州自動車省は、2003年に顔認証を採用し、追加の運転免許証を偽名で申請している人々を検出しました[663]。  
ベースラインとして、2001年に英国国立物理研究所（NPL）が多数の生体認証技術を使用して行ったテストでは、顔認識がほぼ最悪であることがわかりました。単一試行の等誤り率はほぼ10％でした[1217]。  
 顔認識は、ICAOによって、チップが埋め込まれたパスポートとIDカードの標準として採用されました。虹彩コードと指紋はオプションの追加機能でした。  
セキュリティエンジニアリング527ロスアンダーソン17。  
 顔認識しかし、2012年にニューラルネットワークの革命が始まって以来、顔認識のパフォーマンスは著しく向上し、エラー率は桁違いに低下しています。  
 しかし、データはどうですか？おそらく、NISTの顔認識ベンダーテスト（FRVT）によるもので、何百万もの法執行機関のマグショット、刑務所のウェブカメラ画像、野生の写真に対して、1対1の検証、1対多の身元証明、顔の形態検出、顔をテストします。画質評価。  
 最も正確なアルゴリズムは、存在する場合、一致するエントリを見つけます。ギャラリーには1200万人が含まれ、ミス率は0に近づきます。  
 いくつかのアルゴリズムは、サイドビューの写真を正面の写真のギャラリーに正しく一致させます。このような姿勢の不変性は、顔認識研究において長い間求められてきたマイルストーンです。  
 U  
が開発したアルゴリズムでは、アジア人、アフリカ系アメリカ人、アメリカ人インディアンの1対1のマッチングで偽陽性率が大幅に高くなりましたが、1対多のマッチングでは、アフリカ系アメリカ人の女性が最も高率でした。  
 残りのエラーの大部分は、長時間の経年変化、顔の怪我、画像品質の低下、またはTシャツにプリントされた顔などのショットの2番目の顔です[828]。  
どちらのタイプの人間の専門家も対照グループよりもはるかに優れており、2015年から2017年の間に開発された4つの深いCNNは人間の専門家の範囲内で顔を特定し、最新のスコアは法医学専門家の中央値を上回っています。  
内部では、Guodong GuoとNa Zhangによる2019年の調査論文で、顔画像の分析と認識におけるディープラーニングの使用を調査し、システムがポーズ、年齢、照明、表現の変化をどのように処理するかについて説明しています[834]。  
g。  
 メイクや顔の表情を修正するメカニズムもあるかもしれません。  
 しかし、静止画像をビデオに、可視光画像を近赤外にマッチングする場合と同様に、ビデオ画像のぼやけは依然として重大な問題です。  
 また、物議を醸している。  
3。  
 これは中国のビジョンのようです。企業には、個人だけでなくグループも認識するためのトレーニングカメラがあり、分類担当者は、対象者が民族のウイグル人チベット人のように見えるかどうかを警告します。  
 ロシアはそのカメラを使用してコロナウイルス検疫命令を破っている人々を発見しており、そのうちの178,000を配備したと主張している[1907]。  
 これらの企業は、より幅広いサービスを提供するように設定されているようです。彼らは拡張現実の眼鏡のユーザーが、彼らが見ているほとんどの人を識別できるようにする可能性があります-地下鉄の魅力的な見知らぬ人でも、デモでの抗議者でも。同社の支持者は、「法律は合法的なものを決定する必要がありますが、技術を禁止することはできません。  
」[897]。  
 イリノイ州エヴァンストンの家族は、2005年にFlickrにアップロードした子供の写真が、MegaFaceと呼ばれるデータベースに保存され、多くの新しい認識システムのトレーニングに使用されていたことを発見しました。  
 その結果、ソーシャルメディアの顔タグ機能の一部は、イリノイ（または、テキサス）でも機能しません[898]。  
 犯罪者の顔写真を使ってシステムをトレーニングすると、通りすがりの人を見て「この強盗は最も近いマッチだ」と言うことができます。  
 2019年5月、サンフランシスコは交通機関や法執行機関などの政府機関による顔認識の使用を禁止しました。  
 ACLUは、アマゾンのシステムが、逮捕された人々のマグショットに対して28人の議会メンバーの誤った一致を生成したことを示していました。  
 テクノロジーは今やコモディティとなっているので、ビッグ4の自制心は、第2層の企業がそれを販売することを止めるものではありません。  
 裁判所はすでに関与している：2020年8月、ロンドンの控訴裁判所はサウスウェールズ州警察による顔認識の使用がプライバシー権、データ保護法、平等法に違反していることを認めました[1592]。  
 2017年、AppleはそれをiPhone Xに導入しました。ドットプロジェクターはあなたの顔を数万のドットでペイントし、カメラがそれらを読み取ります。  
4。  
 しかし、私の最年長の孫娘のiPhoneは彼女の若い兄弟の両方でロック解除でき、これは家族にとって一般的な問題です[526]。  
4指紋自動指紋識別システム（AFIS）は何年も前から存在しています。  
2005年までに15億3,900万ドルの5％2。  
 尾根の皮膚の毛穴を見ることもある[1213]。  
 マーク・トウェインは、ミシシッピでの1883年の生活の中で、刑務所長であったフランス人の老人からそれらについて学んだと主張する拇印について言及しています。彼の1894年の小説Pudd’nhead Wilsonは、アイデアをアメリカで人気にしました。  
 彼らはまた、何世紀も前にインドで使用されました。  
現代の最初の体系的な使用は、1858年からインドで、天文学者の孫であり植民地の治安判事だったウィリアムハーシェルによって行われました。  
日本の医療宣教師であるヘンリー・フォールズは、1870年代に独立してそれらを発見し、犯罪現場からの潜伏プリントを使用して犯罪者を特定するというアイデアを思いつきました。  
 ゴールトンはネイチャーで記事を書いた[738]。これにより彼は引退したハーシェルと連絡を取り、そのデータにより、ガルトンは指紋が人の生涯にわたって存続することを確信しました。  
 インドの歴史はチャンダク・センゴプタによって伝えられ、その本はまた、フィンガープリンティングが2つのやや疑わしい帝国の制度、すなわち年季労働者制度とアヘン貿易を救ったと指摘している[1701]。  
 彼は1900年に、アシスタント、Azizul HaqueとHem Chandra Boseとともに開発したループ、渦巻き、アーチ、テントのより単純でより堅牢な分類について書いた本を書きました。2指紋印刷技術が現在バンドルされているため、2019年の比較可能な図はありません。 Aadhaarなどのシステムでは、電話または他の生体認証を使用します。  
4。  
 同じ年に彼はロンドンの警視庁長官になり、そこから技術が世界中に広まった3。  
被疑者の10の指のそれぞれに渦巻き（一種の円形パターン）があるかどうかに1ビットを割り当てることにより、指紋ファイルを1024のビンに分割しました。  
 その間、ブリテンハドは有罪判決を受けた重罪犯をオーストラリアに送るのをやめたので、以前の犯人を特定し、彼らがより長い刑を宣告できるようにする必要性が認識されました。  
17。  
1肯定的または否定的なアイデンティティの主張を検証する今日のアメリカでは-19世紀のイギリスのように-かなりの数の犯罪者が名前を変更し、刑務所から解放されて新しい場所に移動します。  
FBIは、この目的のために次世代識別（NGI）サービスシステムを維持しています。 1か月あたり約8千人の逃亡者を特定します[1809]。  
 1日に最大10万回のチェックが行われ、約100万の連邦、地方、および州の行政機関がアクセスできます。  
 国土安全保障省のIDENTシステムは、米国の港に到着した2億人の外国人の指紋を保持しています。世界中の警察や諜報機関の助けを借りて編集された悪者の監視リストと照合します。もう1つのタイプは、システムがIDへの要求をチェックする場所であり、主な米国のアプリケーションは入国管理と福祉の支払いを構築しています[588]。  
 インドには現在、ほとんどの居住者の指紋と虹彩コードを備えた国家システムAadhaarがあり、最初は福祉の支払いをサポートし、誰も2度請求できないように設計されています。  
3スペイン語版の歴史では、彼らはアルゼンチンで最初に使用され、1892年に殺人の有罪判決を受けた。一方、1907年にフィンガプリント局を設立したキューバは、1911年にイリノイで最初の有罪判決を受けた米国を破った。  
ドイツ語版は、1828年に指紋について書いたブレスラウのプルキンエ教授を指しています。  
4。  
 彼らはこれが小切手詐欺を約半分に削減することを発見しました。  
 これらのアプリケーションは認証ではなく、後で悪いことが判明した顧客を特定し、阻止するための試みです。別の例として、バンを借りるときに拇印を要求する英国の大手レンタカー会社があります。  
 したがって、これらは実際には犯罪シーン科学アプリケーションであり、次のセクションで説明します。  
 米国のDHSプログラムが、到着した各訪問者の2つの索引指をスキャンするように設定された後、誤った一致に圧倒されました。  
31％、見逃した一致率は4％[2027]。  
 欧州連合は2020年から4枚のプリントと顔認識の組み合わせを採用する予定です。非居住者は入国するか、どちらかを出て行く必要があります。  
 優れたシステムは、指ごとに1％をわずかに下回る同じエラー率を持っています。  
 逃亡者を阻止するのに十分な確率で高い確率で（そして、管理可能なレベルで誤警報を維持することを意味して）逃亡者を見つけるには、いくつかの指を一致させる必要があります。  
 これは、2010年代のインギャンと米国外での経験とほぼ同じです。  
 追加の構築と設置のコストは、ハードウェアとソフトウェアに費やされたあらゆるものを圧倒します。  
）エラーは均一に分散されていません。  
 自動化されたシステムには、切断者、余分な指など先天性欠損症のある人、および従来の指紋パターンがまったくないまま生まれた（まれな）人の問題もあります[1120]。  
 私がこの指を1989年にFBIがエントリーコントロールを構築するために使用したシステムに提示したとき、私の傷がスキャナーをクラッシュさせました。  
）指紋認証システムは、さまざまな方法で攻撃される可能性があります。  
4。  
最初の重要な技術的攻撃は2002年に行われたときであり、松本勉氏らは、フィンガープリントをクッキングゼラチンを使用して迅速かつ安価に成形および複製できることを示した[1246]。  
 これにより、ドイツのコンピュータ雑誌C’Tは、ハノーバーで開催されたCeBIT電子見本市で販売される多数の生体認証デバイス（9つの指紋認証リーダー、1つの顔認識システム、1つの虹彩スキャナー）をテストするようになりました。  
 潜在的な指紋は、粘着テープを使用して再アクティブ化または転送することもできます。  
2013年、AppleはiPhone 5Sに指紋スキャナーを導入し、他の電話メーカーもそれに倣って競争しました。  
 電話のスキャナーは通常、登録時に8〜12の部分印刷を保存し、それらのいずれかに対してロックを解除します。これにより、スキャナーはより使いやすくなりますが、脆弱になります。  
 2017年、前述のようにAppleは指紋から顔認識に移行しましたが、ほとんどのAndroidOEMは依然として指紋を使用しています。  
他の角度もあります。  
 そして、政府機関がますます多くの版画を収集するにつれて、彼らはますます私的ではなくなります。  
S  
2。  
）指紋認証システムも、ゴルフクラブの駐車場への入場から学校図書館での自動貸出に至るまで、低保証アプリケーションに急速に拡大しています。  
）そしてlatesttwistは、ソーシャルメディアに投稿した写真から人々の指紋を収集するソフトウェアを開発したMitreプロジェクトからのものです。これらはしばしば、FBIデータベースとの照合を得るために指の詳細が不十分であることを示しています[321]。  
 福祉の請求者を認証するために使用される安価な指紋リーダーは5％ものエラー率を持っていますが[383]、そのような効果的な方法であることが判明しましたセキュリティエンジニアリング533ロスアンダーソン17。  
 90年代に採用された福祉ロールを次々と削減するフィンガープリント[1315]。4。  
犯罪現場で見つかったプリントはデータベースのレコードと照合され、特定のレベル以上に一致するものは、容疑者が犯罪現場を訪れた証拠と見なされます。  
 多くの国では、指紋はすべての市民とすべての居住外国人から要求されます。  
 品質と手順のルールは国によって異なります。  
ギリシャは10、トルコ8を受け入れますが、米国には制限がありません（代わりに試験官を認定します）。  
英国では、指紋の証拠はほぼ1世紀もの間、成功を収めることはできませんでした。 16ポイントの指紋の一致は、ぶら下がっている証拠と見なされました。  
 スコットランドの警察官であるシャーリー・マッキーは、スコットランドの犯罪記録局の4人の審査官によって検証された、必要な16点の指紋照合に基づいて起訴されました。  
 彼女は証言を提出した2人のアメリカの審査官を呼んで、それは本人確認ではないと述べた。  
1。  
1：マッキー事件の版画セキュリティ工学534ロス・アンダーソン17。  
 FINGERPRINTS彼女は無罪となり、それが何年も続いた政治ドラマにつながった[1272]。  
 恐ろしい殺人の現場での誤認された印刷物の存在を説明するために、多くの上級警察官が彼女に偽の声明を出すように説得しようとしました。  
 彼女の無罪判決は、彼女の特定の事件だけでなく、より一般的には、警察の証言の信頼性に疑問を投げかけた。  
 政府は、他の訴訟ではさらに数十件の控訴の見通しでパニックに陥り、偽証のために4つの指紋専門家を起訴した。  
 問題はスコットランド議会に何度も戻った。  
 最終的に彼女は政府から750,000ポンドの補償金を獲得しました[189]。  
 米国での注目度の高い2つのケースは、Stephan Cow-ansとBrandon Mayfieldでした。  
 DNAは一致しませんでした。ボストンと州の警察に指紋を再分析させたところ、結局は一致していないことがわかりました。  
 彼らの試合を「絶対に議論の余地がない」と呼んでいたFBIは、2006年にメイフィールドに200万ドルを支払うことで合意しました。  
 審査官の3人は、印刷が一致しないと判断し、その理由を指摘しました。 1つは不明でした。そして、彼らは一致したと主張した。  
 版画はメイフィールドセットではありませんでしたが、いずれの場合も、審査官自身が最近の刑事事件で一致させたペアでした[586]。  
 一貫した専門家は2人だけでした。他の4人は、それらの間で6つの矛盾した決定をしました。  
検察官と警察は、FBI技能試験のエラー率が約1％[205]である場合、法廷での結果に誤りがないことを陪審員に主張し、誤解を招くコンテキスト情報により、これが最大で10％、場合によっては50％を超える可能性があります。  
•図17。  
 したがって、間違いはかなり起こりやすく、審査官のスキル（および偏見）は、マッキー事件、メイフィールド事件、およびセキュリティエンジニアリング535ロスアンダーソン17までに受け入れられたよりもはるかに大きな方法で方程式に入ります。  
 FINGERPRINTS彼らが引き起こした一般的な騒動。  
しかし、法医学の文化は、確実性のみが許容されるようなものでした。最大の法医学グループである国際身元証明協会は、「可能性、可能性、または可能性のある識別について証言する必要がある」と証言した。  
。  
」[205]•警察の楽観主義者が主張するように、16点での誤一致の確率が10億分の1（10-10）であったとしても、多くの印刷物が互いに比較されると、確率論が食い始めます。  
 遅かれ早かれ、16ポイントの不一致を見つけるために十分な一致が行われることは避けられませんでした。  
 欧州の警察部隊が生体認証データベース（指紋とDNAの両方）をリンクして、警察部隊がすべてのEU加盟国の一致を検索できるようになったため、事態はさらに悪化する可能性があります[1905]。  
•あらゆるセキュリティメカニズムに間違いがないという信念は、その適切な使用を損なうために必要な自己満足と不注意を生み出します。  
 16は伝統であり、誰もシステムに挑戦したり、公的資金を被告の専門家に提供したりすることを望んでいませんでした。  
 それでも、ランダム化されたマッチングを複数の専門家と使用することは可能でした。しかし、フィンジャープリント局がおそらく5〜10％のケースで弁護側に、4人の専門家の1人が同意しない場合（たとえば）異議を唱えなければならなかった場合、より多くの被告が無罪となったでしょう。セクション12で説明されているMundenの場合と同様です。  
3は、現金自動預金機のセキュリティに関する魚雷の主張を助けました。セキュリティメカニズムが確実であるという仮定により、手順、文化的な仮定、さらには法律が発生して、その最終的な失敗が可能な限り拒否され、それができないときに実際の影響が及ぶことを保証します。もう延期される。  
このリスク回避は、4人が偽証を試みられたときに後退した。  
 指紋は粘着テープを使用して転写でき、元々警察で使用するために考案された技法を使用してモールドを作成できます。  
5。  
 そして、悪人が額装されていなくても、彼は常に彼がそうであったと主張することができます（そして陪審は彼を信じるかもしれません）。  
 裁判官は、査読付きの科学文献を検討する必要があります。また、捜査当局は、厳格な二重盲検試験に彼らの試験手順を提出することを一般的に望んでいないため、フィンガープリントの場合、これは欠けていました。  
 しかし、現在、局の調査で指紋検査のエラー率がゼロであるということは、広くばかげています[1809]。  
5アイリスコード私たちは今、人々を識別する伝統的な方法から現代的で革新的な方法に変わります。  
 最初の研究はエネルギー省によって資金提供され、プルトニウム店などの施設への入場を確保するための最良の方法を求めていたため、この技術は現在、移民から福祉までのアプリケーションで使用されています。  
知られている限りでは、すべての人間の虹彩はかなりユニークです。  
 それらのパターンには大量のランダム性が含まれ、フィンガープリントの自由度の数が多いようです。  
 一卵性双生児（および単一の個人の両眼）でもパターンは異なり、一生を通じて安定しているように見えます。  
1993年、John Daugmanはアイデアを機能させる方法を考え出し、虹彩の画像から256バイトの虹彩コードに情報を抽出する信号処理技術を開発しました。  
2）。  
 これは、特徴点の方向付けと分類が正確に計算タスクである指紋スキャナーの場合よりもはるかに簡単です。  
 アイリスコードは、既知の検証システムの中で最も低い誤認率を提供します-米国のセキュリティ省エンジニアリングロス・アンダーソンによるテストでゼロ。  
 IRIS CODESEnergyおよびNPL [1217]。  
 実際には、偽りの拒否率はこれよりも大幅に高くなります。まつげから二日酔いまで、カメラが虹彩を十分に認識できない原因となる可能性があります。  
 さらなる問題は、登録の失敗です。 PassportO�ceの試用版では、参加者の10％を登録できず、黒人ユーザー、60歳以上、障害者の方が率が高かった。  
2：–アイリスコード付きのアイリス（提供：John Daugman）アイリススキャンの実用的な問題の1つは、煩わしすぎずに画像を安く取得することでした。  
 協力的な被験者はビデオカメラから数インチ以内に目を置くことができ、最高の標準的な機器は2〜3フィートの距離まで機能します。  
 自動顔認識機能、パンおよびズームを備えたより洗練されたカメラを考えると、旅客が廊下を歩いているときに航空旅客から虹彩コードをひそかにキャプチャすることが可能になり[1240]、2011年に主要な特許がなくなった後、コストが下がった。  
 亡命者たちは、数週間後、汚職によって取得された特定のアジア諸国からの完全に有効な新しいパスポートを持ち帰ります。  
6。  
最大の配備はインドのAadhaarシステムで、その下ですべての居住者が指紋と虹彩をスキャンしました。  
 プロジェクトの最初の動機は、貧困線以下で生活し、福祉を得ている3億人のインディアンが都市に移動して仕事を求めることを可能にすることでした。  
システムは2011年から2016年の間に10億人を登録し、すべての虹彩コードは一意性について互いにチェックされました。  
虹彩認識システムへの攻撃の可能性には、少なくとも無人操作では、標的の虹彩の簡単な写真が含まれます。  
5 Hz。  
最も長くアクティブに使用されているシステムは、虚偽の書類を持って帰国する強制送還者を検出するためのUAEのシステムです。  
Aadhaarと同様に、主な虐待や紛争は、システムを介してではなく、システムの周りで発生します。インドの最高裁判所は、登録されていない人々からのサービスを差し控えるべきではないと判断しましたが、これにより、銀行口座の開設、電話またはSIMカードの購入、および学校への入学のために、登録が実際に必須であることが止められました。  
 それらだけでも、誤認ゼロで自動認識の目標を達成できます。  
6音声認識とモーフィング音声認識（話者認識とも呼ばれます）は、短い発話から話者を識別する問題です。  
 認識がテキストに依存するかどうか、環境が騒々しいかどうか、操作がリアルタイムでなければならないかどうか、スピーカーを確認するためだけに、または大規模なセットからそれらを認識するためだけに必要かどうかなど、多くの副問題があります。  
 フォレンジック音韻論では、タスクは通常、録音された電話と照合することですセキュリティエンジニアリング539ロスアンダーソン17。  
 その他のシステム爆弾の脅威など、いくつかの疑いのあるサンプルからの音声サンプルへの会話。  
 より簡単な生体認証認証の目的は、一部の電話システムで身元の主張を検証することです。  
 英国では、亡命希望者は毎週数回電話をかける必要があります[1902]。  
 私が個人的に使用した唯一のシステムは、私が使用する銀行の1つによって実行されており、電話を変更すると、電話アプリに対して認証されます。  
親戚や悪役がなんとかしてあなたを真似ることができる可能性とはかなり別の、強力な攻撃があります。  
 これは、20年後に現在実行できることと比べると原始的でした。  
 ごく最近、犯罪者はAIを使用して最高経営責任者の声になりすまし、e220,000の支払いを命じました。その詐欺の犠牲者は機械ではなく、別の経営者でした[1841]。  
17。  
 タイピングパターンは1980年代の製品で使用されていましたが、成功したとは思われません（キーストロークダイナミクスとしても知られるタイピングパターンは、無線電信事業者を彼らの最初の使用方法で識別する戦時中の技術の有名な先駆者でしたモールス鍵）。  
 手の幾何学はしばらくの間いくつかの空港で使用され、ベルティロネージュのシステムに歴史的な前身があり、それによって19世紀のフランスの警察は物理的な測定のシステムによって犯罪者を特定しました。  
 これは少なくとも1世紀遡ります。若い男として、有名な暗号学者ウィリアムフリードマンは、ベーコンがシェイクスピアを書いたかどうかを研究するために、風変わりな億万長者によって妻のエリゼベスと一緒に雇われました。  
）コンピューターは、Security Engineering540Ross Anderson17の実行を可能にします。  
 微妙な統計的テストと最新のアプリケーションは、サイバー犯罪市場や過激なWebフォーラムに投稿する人々を特定しようとすることから、大学生による盗用の検出にまで及んでいます[3]。  
 しかし、ほとんどの人はそうではなく、もう少し努力すれば、難読化の試みの事実は通常検出されます[28]。  
その他の提案には、顔のサーモグラム（赤外線画像から得られる顔の表面温度のマップ）、耳の形状、歩行、リッププリント、心電図などがあります。  
 また、食品および飲料業界での品質管理のためのデジタルノーズの開発への莫大な投資は、香りで主人を認識する個人用デバイスにつながる可能性があります。  
 これは、犯罪現場の科学捜査や子供のサポートケースでの親子関係の判断にとって貴重なツールになっていますが、リアルタイムのアプリケーションでは速度が遅すぎて高価です。  
 また、プライバシーに関する問題もあり、DNAサンプルから個人に関する情報を再構成できる可能性があります。  
また、データの品質に関する大きな問題もあります。英国の警察は世界で最大のDNAデータベースを所有しており、600万人近くの記録がありますが、そのうちの約50万人は名前のスペルが間違っていたり、間違っていたりしていました[878]。  
 ローカルポリシングで機能するプロセスは、必ずしも全国規模で拡大するとは限りません。誤入力したレコードから、起訴されなかったために発見されなかった偽の名前を付けた容疑者への小さなエラーは、誤検出率が重大な運用上および政治上の問題になるまで、ラボのエラーと共に蓄積されます。 。これが23andMeや祖先などの大規模な消費者向けDNA企業のビジネスを損なうかどうかは興味深いことです。  
17。  
 セクション3。  
9私は、83か国の5,700の組織に生体認証建物の入退室管理システムを提供している企業が、データベースをオンラインで保護されていないままにしていたとの報告に気付きました。  
 そして、DNAタイピングが直面する主な問題は、不注意な実験室手順のために、最初は高率の偽陽性でした。  
 指紋と同様に、間違いのないものと考えられるシステムは、セキュリティエンジニアリング541ロスアンダーソン17です。  
 WHAT GOES WRONGオペレーターを不注意に壊してしまう。  
。  
）その環境条件が大混乱を引き起こす可能性があるという点で。  
 話者認識のような一部のシステムは、アルコール摂取とストレスに対して脆弱です。  
多くの興味深い攻撃は、生体認証システムに固有であり、複数の種類の生体認証に適用されます。  
 指紋またはDNAサンプルが警察によって植えられた可能性を除いて、それは単に古い可能性があります。  
銀行のドアのプリントは、強盗の金庫のプリントよりもはるかに少ないと言えます。  
 容疑者の版画が銀行のカウンターで発見され、彼が3日前に行ったと主張している場合、支店のカウンターが毎晩磨かれているという証拠で有罪となる可能性があります。  
•鮮度のもう1つの側面は、ほとんどの生体認証システムが、少なくとも理論上は適切な記録を使用して攻撃される可能性があることです。  
 さらに簡単に言えば、指紋が年金の支払いに使用されているSouthAfricaのような国では、「ピクルスの瓶の中のおばあちゃんの指」が、彼女が家族に遺した最も価値のある財産であるという言い伝えがあります。  
 攻撃は必ずしも簡単ではありません。良い指紋から型を作成するのは簡単ですが[406]、人々がドアノブやビールのグラスなどに横に置いたままにしておくカジュアルな印刷物は、識別システムを通過するために汚されすぎて断片的であることがよくあります。  
 防御も可能です。 EU市民が英国のブレグジット後の居住地に申請するために使用するアプリの1つのバージョンは、正面の電話スクリーンの色が変化するにつれて顔のビデオを撮りながら、音声認識システムは、予測できないチャレンジを読み取って録音を阻止するよう要求できますあなたの。  
 高齢者や肉体労働者は、指紋を傷つけたり擦り傷をつけたりしていることがよくあります。ハードコアの犯罪者が故意にこれを行っているという伝統があります。  
 指や目がない障害者は、除外のリスクがあります。  
）「X」を作成する文盲は、署名偽造からより好意的です。  
8。  
 障害者、貧困層、高齢者、民族のマイノリティをなりすましのリスクにさらす、社会的退行性がある（またはそうであると見られる）生体認証システムは、原則として抵抗する必要があります。  
 また、身体障害者のふりをする悪役によっても倒される可能性があります。  
 たとえば、2019年にUK Home Oceは、黒人には適切に機能しないことを知っていたにも関わらず、パスポートアプリを導入しました[1950]。  
 アリスは銀行口座を開き、共犯者のベティはそこからお金を引き出します。その後、アリスは盗難を訴え、水密性を作り出します。  
 彼女は、数週間をかけて自分の庭に壁を作り、指紋をフラットに着用して、指紋システムでの登録を低下させることができます。  
•次の問題は強制です。  
 顔認識を使用している場合、彼らはあなたの頭をピンで留め、あなたの電話をあなたに向けます。抵抗したい場合は、目を閉じて顔を締めます[1348]。  
 たとえば、データベースに10,000の生体認証がある場合、約50,000,000のペアがあります。  
 したがって、識別は検証よりもはるかに困難です。  
•統計学のもう1つの側面は、設計者がバイオメトリクスを組み合わせることでエラー率を低くできると想定したときに機能します。  
 yourhomeに2つの異なる盗難警報器を設置すると、誤警報の数が増える一方で、それらが同時に倒される確率が下がります。  
 したがって、test4より正確には1177が重要です。N人のデータベースでの誤ったペアの組み合わせは、N> p1になるとすぐに可能になります。  
チェック：1177人が1177 x 1176/2 = 692,076のペアを作成し、これらのどれもが誤って一致しない確率は0です。500セキュリティエンジニアリング543ロスアンダーソン17。  
 導入前に、システムを実質的で多様な集団に徹底的に適用します。  
 このことから、生体認証データはプライバシー法の観点から個人データではないため、無制限に通過できると主張されています。  
入力画像がターゲットテンプレートにどれだけ近いかを出力する認識機能が与えられた場合、入力面は連続的に変更され、一致が増加します。  
次に、この山登り技術を使用して、指紋に基づくものを含む他の生体認証を攻撃する方法を示しました[25]。  
虹彩のデータは、人の助けを借りない人間とはまったく一致しません。ほとんどの虹彩コードは、人間の目が感知できない位相情報に基づいています。  
 それでも、私たちのエンジニアは、ユーザーを私たちのテクノロジーに適応しなければならない厄介なものとして扱う方が簡単であるとしばしば感じています。  
 たとえば、自動指紋データベースが最も可能性の高い印刷物であると考えているものを引き出し、それを審査官に提示する場合、彼は有利に偏っていないでしょうか？コンピューターが3つのベストマッチと2つの不十分なマッチを与えることにより、審査官の警戒心を絶えずテストすることは、コンピューターにとってより良いことではないでしょうか？それとも、煩わしすぎますか？  
そのため、重要な問題がいくつかあります。  
17。  
 現在、3つのシステムが大規模に導入されています。電話での指紋認証、インドでの虹彩認証、およびMiddleSecurity Engineering544Ross Anderson17です。  
 概要東および顔認識–ニューラルネットワーク革命のおかげで急速に正確になりました。  
バイオメトリクスが非常に広く使用されるようになると、無人操作で偽造のリスクが高まる可能性があります。虹彩の写真、指紋の型、さらには昔ながらの偽造署名でさえ、すべてシステム設計で考慮する必要があります。  
バイオメトリクスは通常、有人運用でより強力です。優れたシステム設計では、人間と機械の相対的な長所と短所が互いに補完し合う場合があります。  
 歴史的に、多くの生体認証システムは、実際に身元を特定するのではなく、効果的な犯罪のほとんどを達成しました。  
研究の問題多くの実用的な研究の問題は、生体認証システムの設計または改善に関連しています。  
顔認識技術が依然として急速に改善し、新しいアプリケーションを見つけていることを考えると、議論はしばらくの間続き、関連トピックに関する技術的研究を推進する可能性があります。  
 車が盗まれたと思われる場合は、コントロールセンターに電話して確認を求めます。  
 Sohereは別のアイデアです。  
ローカルの方言で流暢に言語を話す能力は、アウトグループからイングループを識別する最も普遍的かつ内臓的な方法の1つです。  
 ロボットだけでなく人間にも、スキルだけで習得するスキルがあるので、これは興味深いところにつながりますか？さらに読む英国の指紋の歴史は司令官Gによるものです。  
C.  
セキュリティエンジニアリング545ロスアンダーソン17。  
 要約マッキー事件はイアン・マッキーとマイケル・ラッセラ[1273]による本で説明されています。  
 顔認識については、Guodong GuoとNa Zhang [834]を参照してください。  
 話者認識の科学捜査については、Richard KlevansおよびRobert Rodman [1058]を参照してください。  
 そして、バイオメトリックフォレンジックのエラーは、他のフォレンジック技術に反映されています。米国国立研究評議会からの2009年の報告は、DNA分析を除いて、ほとんどの法医学的手法は、根本的な科学と技術だけでなく、法医学実務の断片化された性質、基準の欠如、不十分なガバナンスにも関連して、さまざまな点で信頼できないことを示しました[1413 ]。  
セキュリティエンジニアリング546ロスアンダーソン