そしてギレアデ人はエフライミテスの前にヨルダンの通路を取った：そしてそれはそうだった、それで、脱出されたそれらのエフライミテスが言ったとき、私は行きましょう。ギレアデの部下が彼に言った、「あなたはエフライム人なのか」。  
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。その時エフライマイトは四十二千人落ちた。  
17.1はじめに  
（アイザックがエサウを体毛で識別しようとしたが、ジェイコブにだまされたとき、または人々が顔でお互いを認識したとき-これについては後で説明します。  
、いくつかの深く根付いたスキルまたは動作（手書きの署名など​​）  
。  
1。  
海外旅行は、国際標準の生体認証旅行書類、米国への訪問者に指紋を付ける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高速化されています。  
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は大幅に改善されました。  
3。  
人々は自分の生活をすべて電話で、または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ため、紛失または盗難にあった電話を煩わしいものから災害に変えるのに頼っています。  
まず、コンピューター時代以前の生体認証技術（手書きの署名、顔の特徴、指紋）について説明し、次にそれらがどのように自動化されているかを説明してから、さらにいくつかの最新の技術を探っていきます。  
17.2手書きの署名  
ヨーロッパはその逆でした。アザラシは中世に使用されていましたが、ルネサンスの後に文字が広まったため、人々はますます文書に同意するために自分の名前を書きました。  
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るため、それらの大部分が置き換えられています。  
米国では、法律により銀行は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。  
店頭での銀行カード取引の多くは、カードの見本の署名を見なくても受け入れられます。そのため、多くのアメリカ人はクレジットカードに署名する手間さえありません1。  
ある実験では、それぞれ144のペアごとの比較を行った105人の専門の文書審査官が、6.5％の文書を誤認していた。  
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]を反映していると考えられています。  
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って認証され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の名前には、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、確立された顧客ではない銀行から借入したお金を使用し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、財産移転に署名するという手順になります。ローン契約を結び、弁護士に連署される。  
 マネーロンダリング防止法の規定。不動産取引に対する税金を徴収するために、不動産購入が書面であるという要件が数世紀前に課されました。  
 特定の方法で公証する必要があるかもしれません。  
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。  
そのため、この弱い生体認証メカニズムは実際にはかなりうまく機能します。実際の問題は、国やアプリケーションによって異なる一連の手続き規則に起因します。セクション26.5.2で、グローバルおよびナショナルコマースにおける電子署名（「ESIGN」）について説明します  
 これにより、すべての加盟国は承認された製品を使用して作成された電子署名を受け入れる必要があります。  
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。  
署名サービスは通常、手書きのふりをすることを想定した、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会社によって、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。小額の小切手はそのまま通過し、異議を唱えるのはアカウント所有者の責任でした。  
。  
1990年代初頭以来、より優れた製品は、以前に登録された標本とキャプチャされた署名を比較できます。  
多くのシステムは、一方を他方よりも優先するように調整できます。  
カーブ上の適切なポイントを選択するのはオペレーター次第です。  
タブレットベースの署名認識システムの場合、等しいエラー率はせいぜい1％です。純粋に光学的に比較すると数パーセントです。  
ただし、小売店などの顧客向けアプリケーションのショーストッパーです。  
したがって、1990年代に戻って、英国の銀行は、1％の詐欺率と0.01％の侮辱率のバイオメトリクスの目標を設定しました。これは、署名検証と指紋スキャン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ている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。  
17.3顔認識  
生物学者は、私たちの認知機能の重要な部分が他の人の顔の特徴や表情を認識する効率的な方法を提供するために進化したと信じています[1604]。  
顔を認識する人間の能力は、多くの理由にとって重要なベースラインです。そのうちの1つは、写真付きIDに依存しています。  
システムにアクセスするためのパスワードまたはスマートカードの問題は、ジョブの申請または銀行口座の開設時に写真付きIDを提示する人物が開始したプロセスのエンドポイントであることがよくあります。  
 簡単な答えは、私たちはそうではないということです。  
彼らは44人の学生を募集し、それぞれに異なる写真が付いた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、髪型などを持っています。  
さまざまな人物のランダムな数百枚の写真の山の中から、調査員は最も被写体に似ている写真を選びました。  
被験者と同じ性別と人種であったことを除いて、ランダムに選択されました。  
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。  
チェックアウトスタッフが「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、経験豊富なスタッフ、十分な時間、およびカードが拒否された場合の恥ずかしさや暴力の脅威がない最適な条件下で行われました。  
実際、多くの店では、盗難カードを手に入れるためにクレジットカード会社が提供する報酬をチェックアウトスタッフに渡しません。  
それでも、クレジットカードの写真で実験した少なくとも2つの銀行は、詐欺の実質的な減少を経験しました[154]。  
そのため、識別コンテキストで人々が顔認識スキルを効果的に使用しない可能性があります。あるいは、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枚の写真を見て得られる情報とは異なる方法で脳に格納されます。  
誤認が誤った投獄の主な原因であると考えられており、20％の証人がIDパレードで間違いを犯しています[2044]-顔を写真と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、それでも良くはありません。試みは19世紀にさかのぼります。そのとき、フランシスガルトンは、顔の測定のためにばね式の「機械式セレクター」を考案しました[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下でカメラを真っ直ぐに見、その顔をファイル上の顔と比較します。  
最も難しいのは監視であり、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ある人を見つけようとする場合があります。  
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の顔を数百人の既知の地元の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、照合されました。  
イリノイ州自動車省は、追加の運転免許証を偽名で申請している人々を検出するために2003年に顔認識を採用しました[663]。  
ベースラインとして、2001年に英国国立物理研究所（NPL）が実施したテスト  
2005年の英国のパスポートオフィスの裁判は、フィールドの条件により近いものであり、ユーザーの69％（および障害のある参加者の48％）しか認識していませんでした。  
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。  
しかし、2012年にニューラルネットワーク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、データについてはどうでしょうか？  
 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製品を1対1の検証、1対多の識別、顔の形態の検出、顔の画像品質の評価に対してテストします。  
。  
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。  
米国で開発され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マッチングで偽陽性率が大幅に高かったのに対し、1対多のマッチングでは、アフリカ系アメリカ人女性の偽陽性率が最も高かった。  
残りのエラーの大部分は、長時間の老化、顔の怪我、画像品質の低下、またはTシャツに印刷された顔などのショットの2番目の顔[828]によるものです。  
、ランダムな人々のコントロールグループ。  
ただし、アルゴリズムと人間の専門家が一緒に作業すると、最良の結果が得られます[1522]。  
ほとんどのシステムはCNNですが、さまざまな改造があります。  
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、ビデオ画像のぼやけは、静止画像をビデオに、可視光画像を近赤外線に一致させるように、依然として重大な問題です。  
また、物議を醸している。  
 突然、CCTVは犯罪現場の科学捜査のためのツールから、リアルタイムの人物認識と追跡を行うツールに変わります。  
これは、コロナウイルスのパンデミック時に必須のフェイスマスクによって中断されましたが、その後再開することは間違いありません。  
西洋でも、すでに路上車両を追跡している自動ナンバープレート認識システムだけでなく、歩行者を追跡するシステムから警察がフィードを受け取るという未来に直面するでしょうか？  
 しかし、法的制限に直面していないため、法執行機関よりも顔のコレクションがはるかに多い企業が存在し、そのサービスは、法執行機関がファイルに口実を持たない人々によって犯された犯罪を解決するのに役立ちます。  
あなたは彼らの名前、彼らが住んでいる場所、彼らがオンラインで何をしているのかを知ることができます。  
確かに、それはディストピアの未来や何かにつながるかもしれませんが、禁止することはできます。」 [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、新しい認識システムの多くをトレーニングするために使用されるMegaFaceと呼ばれるデータベースに保存されていることに気付きました。その結果、ソーシャルメディアの顔タグ機能は、イリノイ（またはテキサス）で機能しません。  
2018年、Googleは顔認識APIを使用が規制されるまでクラウドプラットフォームで利用できないようにすることを決定しました。  
警察がトリガーハッピーである場合、それは殺すことができます。  
2020年6月、人種差別と偏見のある警察による世界的な抗議行動に続いて、Amazonは、法執行機関がRekognitionの顔認識ソフトウェアを利用できるようにするための1年の一時停止を発表しました。彼らの技術は色の人々を誤認することで批判されていました。  
IBMとMicrosoftはまた、顔認証製品の販売を停止すると発表しました[2004]。  
そのため、大手4社は現在、顔認証製品の規制を推進しています。  
最後に、顔認識は特別なハードウェアで強化できます。  
これは化粧、一部のサングラス、顔の毛を扱っており、以前のiPhoneで使用されていた指紋リーダーの5万分の1とは対照的に、100万分の1の誤認率があると主張されていました。  
  
自動指紋認証システム（AFIS）  
1998年には、5000万ドルの生体認証技術の売上の78％を占めていました。これは、2005年までに15億3,900万ドルの43.5％に落ちました2。  
隆起部の皮膚の毛穴を見ることもある[1213]。  
マークトウェインは、ミシシッピ川での1883年の生痕に言及しました。彼は、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しています。彼の1894年の小説Pudd’nhead Wilsonは、この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。  
日本の医学の宣教師であるヘンリー・フォールズは、1870年代にそれらを独自に発見し、犯罪現場からの潜在的なプリントを使用して犯罪者を識別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、フィンガープリントが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。現在、Aadhaarなどのシステムでは、電話または他の生体認証とバンドルされています。  
同年、彼はロンドンの警視庁長官になり、技術が世界中に広まった3。  
容疑者の10本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個のビンに分割しました。  
一方、イギリス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て、彼らがより長い刑期を与えられるようにする必要があると認識されていました。  
、および犯罪現場のフォレンジック（ヨーロッパでの主な用途）  
  
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自分の名前を変更し、刑務所から解放されて新しい場所に移動します。  
 アメリカの警察部隊は歴史的に指紋を使用して逮捕された容疑者を特定し、現在他の機関に望まれているかどうか、犯罪歴があるかどうか、以前に他の名前で注目されているかどうかを判断してきました。  
 この目的のためのサービスシステム。 1か月あたり約8,000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100万人の連邦、地方、州の職員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。世界中の警察と諜報機関の助けを借りてまとめら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]。現在、インドには国民システムのAadhaarがあり、大部分の住民の指紋と虹彩コードがあり、当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。  
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、後で悪いと判明した顧客を特定して阻止する試みです。別の例は、バンを借りるときに指紋を要求する英国の大手レンタカー会社です。  
したがって、これらは実際には犯罪シーンの法医学アプリケーションです。これについては、次のセクションで説明します。  
 大まかな経験則（それと呼ぶかもしれない場合）  
US DHSプログラムは、到着した各訪問者の2つのインデックスフィンガーをスキャンすることに着手した後、誤った一致に圧倒されました。  
プログラムは「10枚のプリント」に移行しました。各訪問者は、3つの連続したスキャンで各手の4本の指、次に両方の親指を提示する必要があります。  
これはすべて、前のセクションで説明した受信機の動作特性である、偽陰性と偽陽性の間のトレードオフに関するものです。  
誤認は、誤認率を低減するために組み込まれた機能（機能の選択における歪みや柔軟性の許容値など）が原因で発生します[1610]。  
 数本の指を一致させる必要があります。おそらく10本中8本です。  
これは、およそ2010年代にアメリカを出入りする際の私の経験です。  
追加の建物と人件費は、ハードウェアとソフトウェアに費やされる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人、および  
子供のころ、リンゴを切りながら左中央の指を切り、その傷跡が半インチほど残った。  
（10年後にもう一度試したところ、問題なく動作しました。）  
古いトリックは、詐欺師が気を散らす（または賄賂）ことでした  
2002年に最初に注目を浴びた技術攻撃は、松本勉氏らが調理用ゼラチンを使用して指紋を迅速かつ安価に成形および複製できることを示したときでした[1246]。  
これにより、ドイツのコンピューター雑誌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ている9つの指紋リーダー、1つの顔認識システム、1つの虹彩スキャナーなどの生体認証デバイスをテストしました。  
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、アップルは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枚の部分的なプリントを保存し、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。  
上記で説明したように、2017年にAppleは指紋から顔認識に移行しましたが、ほとんどのAndroid OEM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、それらはますます私的なものではなくなります。  
セクション2.2.2で説明したOPMハックを介した連邦職員のプリント。）  
（ほとんどのヨーロッパ諸国のプライバシー当局は、学校で指紋スキャナーを禁止しています。英国では許可されており、プライバシーを意識した両親からの反発を引き起こしています[190]）。  
指紋認証システムが成功する最後の理由の1つは、抑止効果であり、これは特に福祉の支払いで顕著になります。  
  
指紋認識の2番目の用途は、犯罪現場の科学捜査、つまりヨーロッパでの主な用途です。  
彼らはしばしば自分で信念を確保するのに十分です。  
法医学的エラー率は近年非常に物議を醸すようになっており、重大な制限は犯罪現場から撮影された画像のサイズと品質です。  
英国はかつて指紋が16点で一致することを要求していました（対応する特徴点）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）。  
これは、米国では、品質の低いプリントで一致が見つかることがありますが、法廷で異議を申し立てることができることを意味します。  
法廷の信頼はマッキー事件[1273]によって打ち砕かれた。  
彼女はそれが自分の指紋であることを否定し、英国の独立した専門家に彼女をサポートしてもらうことができなかったことがわかりました。職業はランクを閉じました。  
犯罪現場とファイルのプリントは、図17.1に並んでいます。  
 犯罪現場のプリント（b）  
最初の問題は彼女に対する訴訟の性質だった[1273]。  
彼女がそうすることを拒否したことで、彼女は信用を傷つける手段として偽証罪で起訴されました。  
その殺人で有罪判決を受けた男は上訴で無罪となり、補償のために警察を訴えた。  
それもどこにも行きませんでした。  
警察はシャーリー・マッキーの復職を拒否し、関係する役員は昇進し、その列はこれまでになく厳しいものになった。  
この事件は、指紋の識別の価値について専門家の間で幅広い議論につながり、指紋の証拠は他の多くの国で首尾よく異議を唱えられた[760]。  
スティーブンコワンズは強盗の後で1997年に警察官を射殺したとして有罪判決を受けましたが、彼の印刷物が誤認であると主張し、DNAの証拠をテストするのに十分なお金を貯めた後、6年後に控訴で無罪となりました。  
ブランドンメイフィールドはオレゴンの弁護士であり、FBIがマドリード爆撃の犯人の1人であると誤って特定し、マドリード警察がより一致する指紋を持つ別の男を逮捕するまで2週間保持しました。  
その後の研究で、心理学者のItiel Drorは5枚の指紋検査官に1組の版画を見せ、メイフィールド事件からのものであると伝え、FBIがどこで間違っているのかを尋ねました。  
彼だけが正しかった。  
Drorは6人の専門家がこれを繰り返し、それぞれが過去8年間に実際に調査した8枚の版画を見ました。  
印刷にはさまざまな困難があり、提供されたコンテキスト情報が誤解を招くケースはわずか半分でした[587]。  
コメントは4つあります。  
だから間違いはかなり可能性があり、スキル（と偏見）  
Drorの研究は、誤認が発生するケースは難しいものである傾向があることを確認しました[587]。  
不道徳な行動をとる。」 [205]•16ポイントでの誤一致の確率が100億分の1であったとしても（10ffi10）  
昔、犯罪現場の印刷物としてうまく機能していたシステムは、手動で数百の既知の地元の強盗の記録と比較され、何千もの印刷物が毎年数百万のオンラインデータベースと比較されると機能しなくなります。 。  
実際、指紋データベースのほとんどの人はシャーリーマッキーが行ったような断固たる抗弁を要求することができない軽犯罪者であるので、他の間違った信念がすでになかったとしたら、私は驚きます。  
 警察がすべてのEU加盟国で一致を検索できるように[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。  
 コンピューターマッチングの導入で20。  
英国ではすべての専門家が警官または元警官だったので、とにかく雇うために利用できる独立者はいなかった。  
 4人の専門家の1人が同意しなかった場合、より多くの被告が無罪となったであろう。  
現金自動支払機のセキュリティに関する魚雷の主張を助けたセクション12.4.3で説明されているMundenの場合と同様に、セキュリティメカニズムが絶対的であるという仮定は、手続き、文化的仮定、さらには最終的な失敗が確実に拒否されることを確実にするための法律を引き起こします。可能な限り長くなるため、延期できなくなった場合に大きな影響を与えます。  
。  
ただし、正しい一致があったとしても、その影響は必ずしも完全に明らかであるとは限りません。  
そのため、犯罪現場で印刷物が見つかった容疑者が別の犯罪者（または警察）によって取り囲まれた可能性があります。ほとんどの偽造事件には、他の容疑者ではなく法執行要員が関与しています[254]）。そして、悪役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）  
米国では、最高裁のドーバート判決において、裁判官は法医学証拠の背後にある原則と方法論をスクリーニングして、関連性と信頼性を確保する必要があると判断しました[516]。  
法医学指紋証拠に関連する多くのドーバート公聴会が米国の裁判で開かれており、FBIが一般的に勝訴している[761]。  
  
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。  
。  
妊娠3〜8か月目に形成され、（指紋パターンと同様に）  
一卵性双生児でも（そして単一の個人の2つの目でも）パターンは異なります  
Leonard FlomとAran Safirは、1987年に虹彩識別システムのアイデアの特許を取得し、すべての虹彩が異なることを確認しました。  
これには、瞳孔と虹彩の外側との間の同心リングの数で行われる円形ウェーブレット変換が含まれます（図17.2）  
結果のアイリスコードは、同じアイリスから計算された2つのコードが通常、ビットの90％で一致するという明確な特性を備えています[517]。  
アイリスコーディングの速度と精度、およびドーグマン特許の期限切れにより、多くの商用アイリス認証製品が生まれました[1996]。  
等しいエラー率は100万分の1よりも優れていることが示されています。1万分の1の偽の拒否率を許容する準備ができている場合、理論上の偽の受け入れ率は1兆分の1未満になります。  
米国国防総省は、2002年の実地裁判で6％の偽棄却率を発見しました[1258]。英国のパスポートオフィスの裁判では、通常のユーザーが4％、障害のあるユーザーが9％でした[1920]。  
図17.2：–アイリスコード付きのアイリス（提供：John Daugman）  
アイリスが小さい（1/2インチ未満）  
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。  
自動化された顔の特徴認識、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。  
亡命者は、数週間後、汚職によって入手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。  
最大の配備はインドのAadhaarシステムで、すべての居住者が指紋と虹彩をスキャンしました。  
この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3億人のインド人が、仕事を求めて都市に移動できるようにすることでした。  
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。  
しかし、広く販売されている安価な端末はこれを行わず、活性検出が広まった場合、攻撃者はターゲットの虹彩パターンをコンタクトレンズに印刷するなど、より洗練されたトリックを試すでしょう。  
典型的な攻撃は、帰国する強制送還者が飛行機でアトロピン点眼薬を服用し、瞳孔を拡張することでした。今日、そのような旅行者は、目が通常に戻るまで監禁されています。  
2019年のホットな問題は、当局がアッサムおよびその他の国境地域でムスリムを登録することを躊躇していることであり、彼らを不法移民として描写しようとするより大きな政策の一部です。  
困難にもかかわらず、アイリスコードはある意味で最も強力なバイオメトリックであり、正しい状況では、目の前の個人が最初にアイリスが登録された人物と同じ人間であることを保証します。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ある必要があるかどうか、スピーカーを確認したり、大規模なセットからそれらを認識するだけでよいかどうかなど、多くの副問題があります。  
フォレンジックフォノロジーでは、タスクは通常、爆弾の脅威などの録音された電話での会話を、多数の疑いからの音声サンプルと照合することです。  
より簡単なバイオメトリック認証の目的は、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、庇護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つによって運営されており、電話を変更すると、電話アプリに対して認証されます。  
親族や悪者がなんとかしてあなたを真似する可能性があるという可能性とはかなり離れて、いくつかの強力な攻撃があります。  
これは、20年後の現在と比べて原始的でした。  
ごく最近では、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]。  
  
他の多くの生体認証技術が提案されている[1315]。  
。  
。  
文体学、つまりテキストであろうとコードであろうと、著者の作文スタイルから作者を識別する科学への関心が最近高まっています。  
（彼らは最終的にアイデアを覆しましたが、その過程で暗号に興味を持ちました。）  
研究者は、人々がそれらを試せば、人々は単純な文体測定を打ち負かすのに十分な書き方を変更できることを示しました[318]。  
文体測定はコードにも拡張されます。プログラマーはコーディングスタイル[370]から認識できます。  
、耳の形状、歩行、リッププリント、心電図。  
そして、おそらく食品および飲料業界での品質管理のためのデジタル鼻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かもしれません。  
これは、犯罪現場の科学捜査や養育費事件における親子関係の判断のための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には非常に遅く、高価です。  
また、プライバシーに関する問題もあり、DNAサンプルから増加する個人に関する情報を再構築することが可能です。  
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データベースを持ち、約600万人の記録がありますが、そのうちの約50万人の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。タイプミスしたレコードから、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、偽陽性率が深刻になるまで、ラボのエラーとともに蓄積されます。運用上および政治上の問題。  
これが、23andMeやancestry.comなどの大規模な消費者向けDNA企業のビジネスを弱体化させ、より強力なプライバシー法を求めるロビー活動を行うのに十分かどうかは興味深いことです。  
17.8間違ったこと  
セクション3.4.9で、83か国の5,700の組織に生体認証ビルディングエントリーコントロールシステムを提供している会社が、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たという報告に触れました。  
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、最初は高い率の偽陽性でした。  
指紋と同様に、絶対的であると考えられているシステムは、オペレーターを不注意に破壊してしまいます。  
 その環境条件で大混乱を引き起こす可能性があります。  
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見つかり、3日前に行ったと主張した場合、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、南アフリカのように年金の支払いに指紋が使用されている国では、彼女が家族に残した最も価値のある財産である「おばあちゃんの漬物瓶の中の指」のしつこい物語があります。  
攻撃は必ずしも簡単ではありません。良い指紋[406]からカビを作るのは簡単ですが、ドアノブやビールのグラスなどに人々が横に置いたままにしておくカジュアルな印刷は、多くの場合、汚れて断片的で、識別システムを通過できません。  
防御も可能です。 EU市民が英国のブレグジット後の居住を申請するために使用するアプリの1つのバージョンは、電話で色が変化するにつれてあなたの顔のビデオを撮りましたが、音声認識システムは、録音を阻止するための予測できない課題を読み取ることを要求できますあなたの前のスクリーン。  
。  
暗い目と大きな瞳孔を持つ人々は、より弱い虹彩コードを与えます。  
（それがAadhaarが虹彩と指紋の両方を使用する1つの理由です。）  
生体認証エンジニアは、そのような対象を「ヤギ」と非難して呼ぶことがありますが、これは愚かで差別的です。  
 社会的に退行的で​​あり、それにより障害者、貧困層、高齢者、民族の少数者がなりすましのリスクが高くなるため、原則的な抵抗に会うべきです。  
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年に英国の内務省はパスポートアプリを導入しましたが、パスポートアプリは黒人には適切に機能しないことがわかっていました[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、水密アリバイを作成します。  
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は、頭を固定してスマートフォンをあなたに向けます。抵抗したい場合は、目を閉じて顔を伸ばしてください[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場合に役立ちます。  
自宅に2つの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可能性が低くなります。  
したがって、4177を正確にテストすることが重要です。N人のデータベースでの誤一致ペアリングは、N> p 1.386 / fになるとすぐに可能になります。ここで、fは単一の誤一致率です。ここでは10ffi6 [519]です。  
•保存されるのはあなたの顔や指紋や虹彩の画像ではなく、それから派生したテンプレートであり、一方向のハッシュのようなものであり、そこからはできないため、多くのベンダーは自社の製品がプライバシーを保護すると主張しています識別されます。  
これらの主張は、顔認識システムに対する興味深い山登り攻撃を考案したアンディアドラーによって爆発しました。  
テストされたシステムでは、これによりターゲットの認識可能な画像が急速に得られました。そのプリントアウトはターゲットの顔として受け入れられます[24]。  
•人間とコンピュータが一致しない場合に何が起こるかを考える価値があります。  
しかし、ガードとプログラムが、被写体の顔がファイルの写真と一致するかどうかについて意見が一致しない場合はどうなりますか？  
それでも、私たちのエンジニアは、ユーザーを私たちの技術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だと気づくことがよくあります。  
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、彼はその傾向に偏っていないでしょうか？  
 •最後に、キリスト教原理主義者はバイオメトリクスに不安を感じています。  
しかし、バイオメトリクスは今や主流になり、優れたセキュリティエンジニアは、バイオメトリクスを適切に使用する方法を知る必要があります。  
17.9まとめ  
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、インドと中東での虹彩認証、および顔認証です。これらは、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。アイリス、指紋のカビの写真、さらには昔ながらの偽造された署名でさえも、システム設計ですべて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、実際に犯罪者を特定するのではなく、犯罪者を抑止することによってその効果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。  
これが別のアイデアです。  
 たとえば、この章の冒頭にある引用–エブラマイトがヘブライ語の文字「シン」を言うことができないために発見されて殺された–は実際には、人々が若いとき、または大人としてより困難なときに学ぶスキルに関するものです。  
クールな群衆は、最新のスラングを話し、最新のダンスを踊ります。  
 参考文献イギリスの指紋の歴史は、司令官G.T.Cによるものです。  
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。  
顔の認識については、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。  
 顔認識からDNAまでの複数の形態のバイオメトリクスを含み、米国の居住者と外国人の両方の記録を統合するデータベース。 EFF [1196]によるポリシーの影響の説明と議論があります。  
最近の例として、ソフィーナイチンゲールとハニーファリッドは、縫い目パターンによってデニムの服を特定する一般的な方法は、法医学調査官が長年主張してきたほど信頼性や再現性が低いことを発見しました[1447]。