

人脸识别门禁。

BOON EDAM发表的《白皮书》

BOON EDAM
YOUR ENTRY EXPERTS.



简介

本《白皮书》解释了人脸识别门禁的工作原理。还讨论了在选择人脸识别门禁系统时应考虑的因素。由于人脸识别技术面世的时间还不久，您可能想知道哪些方面可以在应用中发挥作用。阅读本《白皮书》可以让您更深入地了解人脸识别门禁的具体要求，以及在购买这种系统时应该考虑什么。

生物识别类型

生物识别码是可用来描述人类的所有可测量特征。生物识别在门禁应用中越来越受欢迎。以下是四种最常见的形式：

虹膜扫描

每个人的虹膜都有独特的特征。虹膜扫描仪可识别虹膜上的凹陷孔、卷缩沟和条纹，并将它们转换成虹膜代码。随后将此代码与数据库进行比较，确定是否允许出入。

手掌静脉

近红外照明可显示手掌独特的静脉和毛细血管图案。一些手掌扫描仪还可以测量像掌纹和结节这样的特征。此信息可创建链接到授权人员的唯一个人资料。

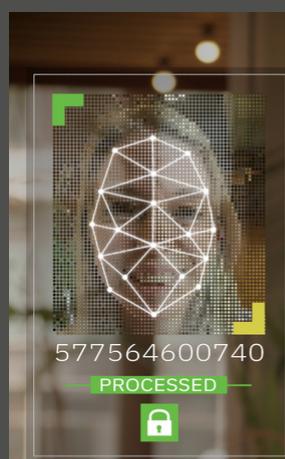
指纹

现有各种类型的指纹扫描仪。它们的工作原理都是记录皮肤上独特的纹路。结果数据可用于确定是否允许出入。

人脸识别

最后一种类型的生物识别门禁采用人脸识别技术。一种用于从视频或照片图像中过滤人脸的算法。在短短几毫秒内，就能记录人脸的特征，并转换成一种独特的代码。

然后人脸识别软件将代码与数据库进行比较。如果找到匹配，就可以用来识别图像中的人员，用于确定是否允许出入。





人脸识别

人脸识别在很多方面都有用武之地。本《白皮书》主要关注它在门禁方面的应用。下面简要讨论应用领域之间的差异。

大规模监控

大规模监控使用人脸识别从人群中识别出个体人员。这需要专门的硬件和强大的软件才能实现。

个人身份验证

这种类型的人脸识别通常用于智能手机等移动设备，软件和硬件要求相对较低。在这些应用中，人脸可替代密码。

事故调查

人脸识别也可用来基于视频图像重建个人路线。例如，这些数据可以帮助确定逃犯在过去 24 小时内的位置。

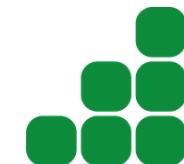
门禁

最后，人脸识别可用于门禁系统。很重要的一点是，要设置软件来实时比较多个摄像头和数据库中的信息。根据数据库的大小安装一台服务器，尽快验证授权，然后就可以打开出入点。

在本《白皮书》中：



人脸识别的优势



人脸识别的组成部分



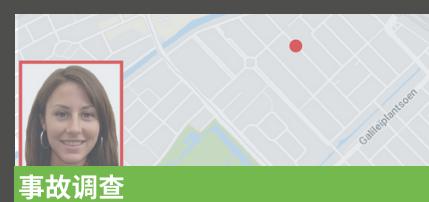
技术因素



实际应用



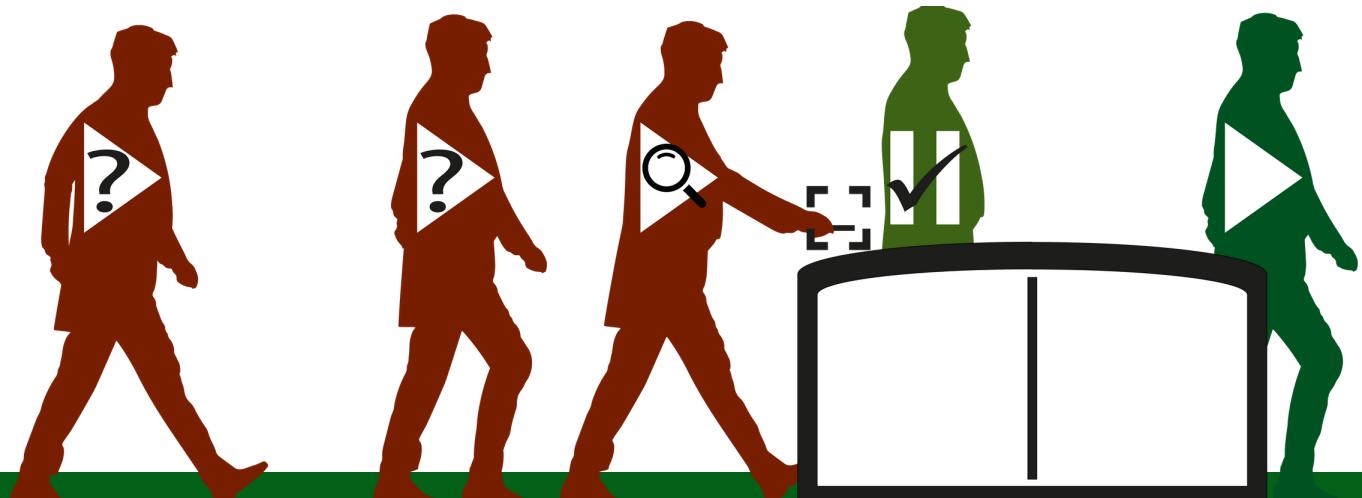
数字安防



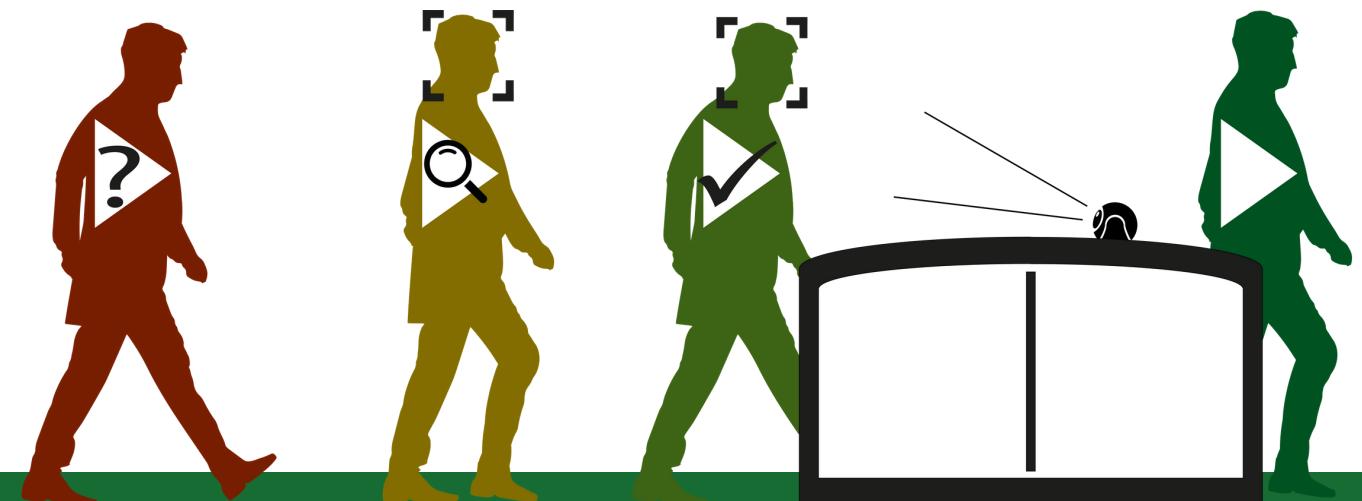


人脸识别的优势

“传统”读卡器



人脸识别



改善流量

人脸识别门禁的主要优势之一是无需在出入点等待。当一个人靠近时，该软件会记录其脸部信息，并决定是否允许其在到达门口时出入。当被授权人员接近或抵达出入点，系统会打开门。这样就可以防止混入未经授权的人。此外，该人员可以顺利通过出入点。



随时都能快速出入

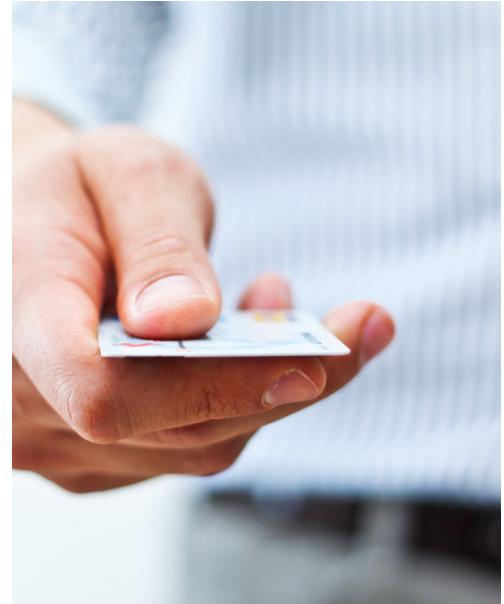
因为人脸识别是基于人们自身的生物特征进行识别，因此紧闭的门始终会为他们而开。每个人的脸都是独一无二的，人们由此可以彼此区分，并通过面部特征来识别身份。

另一个优势是，用户在门禁附近只需主动进行少量操作。只要人脸进入摄像头的焦距范围，软件就可以检查授权。由于不再需要通行证，也就不存在忘带通行证这种事情啦。此外，无需等同事翻找通行证，双手也可以腾出来拿外套和手提包。

请勿共享通行证

使用门禁过程中与同事共享个人通行证的情况普遍存在。这种不当使用可能导致未经授权的人员进入场所。使用人脸识别可防止陌生人以这种共享方式通过门禁系统。

此外，采用人脸识别门禁不会再发生盗取或复制通行证的情况。最终能提高总体安防级别。



非接触式生物识别技术

许多人在扫描虹膜或手指前会犹豫片刻。他们（潜意识中）的犹豫是因为对系统不熟悉，或者不愿意主动向扫描仪展示身体部位。这样除了中断流程之外，还会导致门禁系统的用户体验变差。

人脸识别的另一个主要优势在于，可以用摄像头从远处记录用户信息。用户不必摆出尴尬的姿势或实际接触出入点。只要他们进入摄像头的识别区域，就能验证身份，从而顺利通过出入点。





人脸识别的组成部分

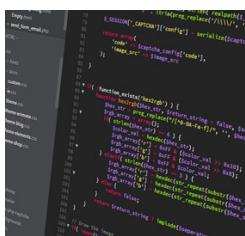
在选择人脸识别门禁时，需要考虑的一点是系统中将会包含多个组件。这些组件通常由多方提供，并且组件必须相互交互。因此，调查哪些供应商可以合作构建一个平稳运行的系统十分重要。一般来说，以下组件需要进行交互：



摄像头和其他传感器

摄像头是人脸识别软件可靠应用的重要组成部分。市场上有各种各样的高质量摄像头。经验表明，基于技术和美学因素慎重选择，有助于提升用户便利度和接受程度。

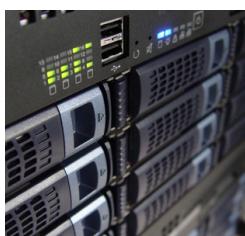
选择过程不仅仅涉及像素；光敏度、镜头类型和芯片的处理能力也是需要考虑的重要因素。也可以选择其他传感器，例如能够区分人脸和照片的传感器。



人脸识别软件

人脸识别软件是系统的核心，能将面部特征转换成代码，与预先建立的数据库进行比较。识别是通过使用一系列算法来实现的。人脸识别软件经常独立于其他形式的门禁软件运行。这就能够创建一个在外部处理器上运行软件的独立系统。

确保软件和系统符合《通用数据保护条例》(GDPR)且具有正确的加密标准十分重要。

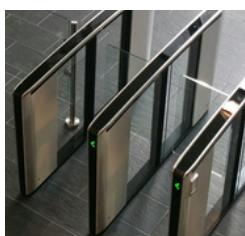


门禁系统

门禁系统通常需要集成多个软件解决方案。

这些解决方案通常与安全管理或建筑管理系统集成。因此，人脸识别软件可能也需要与这样的系统兼容。

在实际应用中，这将涉及到各个模块的链接，通过一个单独的中心程序进行后续控制。在这种情况下，“人脸识别软件”模块将通过 API 进行集成。



实际出入

在门禁应用中，人脸识别通常与实际门禁产品结合使用。毕竟在未设置此种屏障的情况下，不可能阻止未经授权的人员进入。有各种可用的屏障选项，每个选项都有独特的安防级别。

可以以各种方式配置组件。例如，有完全集成人脸识别的实体产品，也可以单独购买组件。



技术因素



光照条件

摄像头所在区域的光照条件是成功进行人脸识别的最重要因素之一。在使用门禁的情况下，通常在室内进行人脸识别，很容易适应光照条件。

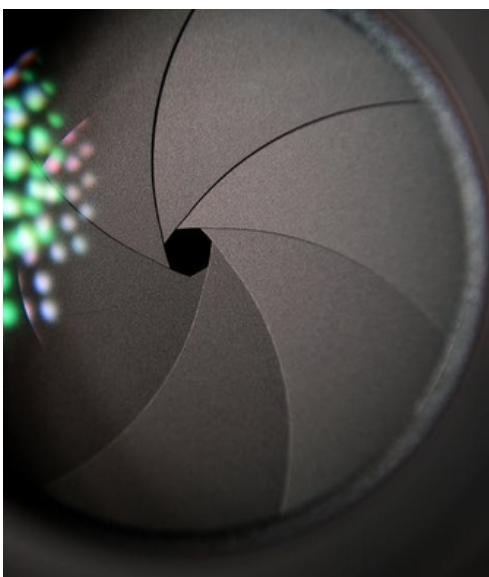
过度曝光是一个真正的挑战。包括耀眼的阳光、反射眩光或高亮的玻璃天花板。对于摄像头和人脸识别软件来说，光照的波动难以控制。曝光不足更容易纠正。通常情况下，调整摄像头设置就足以达到良好的识别效果。建议请专家来进行正确设置。

摄像头安装位置

当安装摄像头时，要仔细考虑记录的图像。摄像头离要出入的人越近，图像的质量就越高。

摄像头的位置也要考虑用户的位置。当用户准备通过出入点时，最好将摄像头放置在用户视线相对的位置。这样一来，他们无需其他动作就能进行识别。

最后，出于美观考虑，最好将摄像头集成到门禁产品中，或者将其安装在外部。



摄像头焦距

安装摄像头时，要仔细考虑焦距。应设置在适合人脸扫描的位置。焦距不能离出入点太远（防止有人溜进去），也不能太近（导致等待）。

摄像头的焦距也决定了人脸识别的范围。可以通过在软件中选择进行人脸识别的图像区域进行调整。

我们的专家将很乐意帮助您根据实际情况选择合适的技术规格。

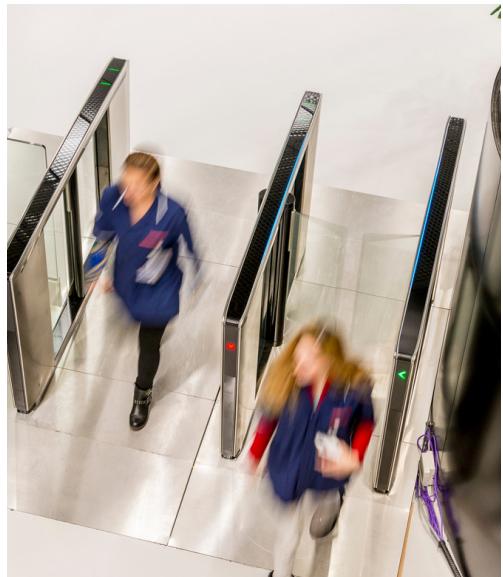


实际应用

用户流量

在实际应用中，速通道的使用会自然而然地引导用户面朝前方。人们将在通道中直线前进，面朝前方。最终进入一个相对较小的区域，所有用户的脸都会通过这个区域。

人脸识别门禁的另一个巨大优势是可改善用户流量。这是因为用户都会朝着相同的方向前行，源源不断地通过速通道。人脸识别可确保验证过程足够快，保持人员快速流动。



呈现用户的脸部

本《白皮书》前文指出，用户无需使用人脸识别门禁进行额外操作。然而，用户必须有意识地让人脸识别软件能够扫描到脸部。

实际上，这意味着用户必须或多或少地正视摄像头。例如，当他们戴口罩或向后看时，是不能通过出入点的。用户必须配合才能使系统正常工作。

与用户交互

在人脸识别的使用以及通用的门禁中，良好的反馈对于用户来说至关重要。当多人快速连续使用一个出入点时，可通过视觉和听觉信号将软件的结果传达给用户。

人脸识别非常适合于有很多重复出入用户的情况。用户登记一次后，就可以根据需要被授予出入权限。重复出入的用户也将逐渐习惯与门禁产品的交互。





数字安防



加密

为了防止通过网络传播的数据和图像轻易被黑客攻击，人脸识别软件使用了加密技术。加密涉及数字（图像）信息的编码。如未能事先了解加密过程，外部人员就不可能读取数据。

可以使用各种数据加密方法。现有的基础设施和（当前的）视频管理软件平台将决定最合适的解决方案。例如，在一个封闭或开放的网络上传输数据是有区别的。我们的专家很乐意回答您关于这个问题的任何疑问。

欺诈检测

在欺诈检测方面，人脸识别技术也在不断发展。其目的是防止系统被“愚弄”，例如，向摄像头出示照片。目前有两种检测和预防欺诈的方法：

- 通过扫描人脸结构的 3D 传感器进行硬件检测。其中涉及记录从一张脸上反射回来的彩色光线图案的传感器。
- 通过提取视频图像中的微小差异进行软件检测。这需要更强的（视频）处理能力，需要更强大的服务器。



GDPR

本《白皮书》前文指出，人脸识别需要使用生物识别数据。在《通用数据保护条例》(GDPR) 的背景下，生物识别数据属于个人数据的一个特殊类别。在某些情况下，此类数据可用作个人身份证明。这些数据仅能用于身份验证或安防目的。此外，系统管理员必须证明数据处理符合此条例。因此，在门禁应用中使用人脸识别是合法的。



结论

本《白皮书》旨在提出一些关于人脸识别门禁的初步见解，以及哪些因素将决定什么人脸识别系统最适合您的公司。它解释了不同类型的生物识别和人脸识别方法之间的差异。此外，它描述了人脸识别与传统门禁系统相比的优势。

我们还介绍了用于门禁的人脸识别系统的各个组件，以及人脸识别系统最重要的技术和实践因素。最后，本《白皮书》简要介绍了人脸识别在数字安防以及当前的 GDPR 条例背景下的应用。

推荐

在本《白皮书》中，Boon Edam 试图[TG1] 为您提供一些关于人脸识别的相关条件和要求的见解。我们相信，人脸识别技术近几年已经证明了它的价值，未来的使用只会越来越广泛。此外，我们想说，人脸识别几乎适用于所有安防级别的门禁系统。根据您对人脸识别的期望以及您的具体情况（例如系统必须识别的人数、出入点的位置等），我们很乐意帮助您选择并实施最适合您需要的系统。

有关人脸识别门禁的更多信息，请联系本《白皮书》的作者或我们的其他专家。我们将很高兴义务为您提供咨询。

常见问题

如果作为用户，我通过人脸识别接近一个出入点，这会对我的面部情况进行编码，然后将它们与数据库进行比较。这是否意味着它将存储我的照片？

并非如此，数据库的创建不需要存储用户的脸部信息；一个哈希码列表就足够了。使用门禁产品也无需存储照片进行比较。然而，在实际应用中，人脸识别装置可能会（暂时）存储照片以优化软件。它们位于独立服务器上，不会与第三方共享。

除了哈希码之外，还有其他数据存储吗？

一般来说，传统的门禁系统会记录获得授权的用户进入场所的时间，人脸识别装置也是如此。可以调整设置以防止此类数据的存储。

这种类型的人脸识别是否适用于除大门之外的其他出入口解决方案？

是的，这种类型的人脸识别也适用于其他的出入口解决方案。我们很乐意与您讨论这些可能性。

我们的业务通达全球

宝盾专注于生产高端、美观且安全的出入口解决方案已超过140年，产品来自荷兰、美国及中国三个生产基地。我们能够自豪的宣布，宝盾的产品覆盖全球每一个角落，分公司能够通达服务于全球的主要城市。

此外，我们不仅通过自身的全球出口部门与经销商合作，而且还直接销售和服务于每一个地区。我们经由这个网络涉足全球，也使个性化定制和符合当地独特需求成为可能。

如您需要获知更多的内容，请登录Boon Edam的官方网站：
www.boonedam.cn/contact



Beijing Boon Edam Entrance Technology Co. Ltd
T +86 (0) 10 67877766
E cn.info@boonedam.com
I www.boonedam.cn

 **BOON EDAM**
YOUR **ENTRY** EXPERTS.