目录

[一、 市场化 1](#_Toc15317015)

[1. 受众广 1](#_Toc15317016)

[2. 使用方便 2](#_Toc15317017)

[3. 成本低廉 2](#_Toc15317018)

[ 方案1： 2](#_Toc15317019)

[ 方案2： 4](#_Toc15317020)

[4. 推广快 4](#_Toc15317021)

[**PS：开源项目如何赚钱** 4](#_Toc15317022)

[二、 未来扩展 5](#_Toc15317023)

[1. 动态识别报警 6](#_Toc15317024)

[2. 人脸识别 6](#_Toc15317025)

[3. 语音识别+智能助手+音频加密 6](#_Toc15317026)

[4. 日志记录并分析 6](#_Toc15317027)

[三. 技术亮点之加密算法 6](#_Toc15317028)

[引用 7](#_Toc15317029)

1. 市场化
2. 受众广

学生宿舍防盗，教师办公室监控，家庭等私人场所的监控，需要监控但是要求安全性较高的场所；

1. 使用方便

因为我们的软件是开源的，用户可以自行购买树莓派和CSI接口/USB接口的摄像头，再租赁一个可用于存储的服务器，即可以实现一个安全可靠的摄像头系统。当然，如果用户无法自行搭建，我们也可以提供相应的服务，从而获取一定的利润；并且该系统只需要接入一个电源即可工作，数据等交互操作都可通过无线网进行；

1. 成本低廉

* 方案1：

树莓派加一个摄像头，基础费用应该不超过五百块钱人民币；如果需要多个摄像头只需要在树莓派上扩展USB接口即可（可扩展性）；

加上每一个月租赁服务器的费用，平均一个月在30元左右（学生价大概在10元左右）；

市场上目前一个摄像头加本地存储的价格为900元左右

以海康威视为例



那么我们在价格上基本上便宜了至少1/3，并且摄像头因为支持用户DIY，那么系统中的摄像头清晰度可以由用户自行选择，可以根据不同的用途来决定摄像头，不用拘泥于同一类型的摄像头；

再者是云存储，即可以在服务期间存储一定时间内的监控视频，以海康威视的萤石云为例：



这些服务一般来说，只能存储一定时间内的活动图像，并不能受用户自行控制，而我们提供的服务，上传到云服务器上的活动图像是永久保存的，他们可由用户自行管理，当然它会受限于云服务器的存储空间；虽然我们的价格优势在初期用户量少的时候，会很小，但是当用户基数多起来之后，云服务器的租赁成本在分摊下来之后自然可以降低，而我们的优势主要在于**用户自主管理的灵活性**；

* 方案2：

我们为一些企业和安全要求较高的用户在原有系统的基础上加上了TPM安全芯片，这个在一般的商用或工业级摄像头中并未使用，因为我们系统中的程序都是自主编程的，TPM主要保证它们不被篡改即可保证安全性，目前市场上的TPM安全芯片价格在450块钱人民币左右，而TCM只需要280块钱人民币左右，在TCM芯片正式推广之后，我们的成本将显著降低；

1. 推广快

项目开源，设备购买渠道广泛，只要懂得搭建该系统的人不仅可以自己搭建，还可以可以将其当作一份兼职，为当地购买该服务的人提供帮助，一方面该兼职人员可以得到工资，另一方面也可以加快我们的产品推广；

**PS：开源项目如何赚钱**

1、先让免费成为习惯，让您离不开，潜移默化了，好用的话也会和朋友推荐，引流就产生了。

2、流量大了，那么就开始拉广告商来了，产生广告效益。

3、软件使用的需求有高低，为了满足各种人群，开始有不同的套餐收费了。

得到用户的认可，有了用户黏度，扩大了开发者的知名度，就能使开发者的其他软件获利 开发者可以通过增值功能来赚钱，比如免费用户使用远程连接等服务有时间和次数限制，而付费用户没有 开发者可以限制软件某些关键功能，只有付费才能使用 当前软件是免费的，如果以后没有类似的软件可以替代，或者其他同类软件的功能上有欠缺，开发者也能将软件转为收费 些软件是需要下载额外数据的，开发者可以通过这些额外数据来赚钱开发者通过收集使用者的信息，通过大数据来赚钱。

这是有公司买过来免费让用户用的。不是开发者免费的。

大家通常想到的就是软件免费、服务收费，可以通过技术支持、二次开发这些方式来收费。

基本模式就是通过开源软件获得大量用户，然后通过专业增强版本的授权实现盈利。

不同的软件、不同的领域有不同的盈利模式，**但所有模式的基础都是用户数。只有用户数量达到了一定的规模，才有成其模式的可能。**

抛开用户数空谈盈利模式，其实是没有任何价值的。

品牌的建立是需要时间的，需要耐心，需要坚持。

盈利手段总结：

1、电子商务

2、广告：广告费+流量费

3、增值服务

1. 未来扩展

加入动态识别报警，人脸识别，语音识别等功能；

1. 动态识别报警

目前市面上的摄像头都开始支持自动报警，只要监控画面中出现异动，就会远程向用户进行报警，这样的摄像头比一般的摄像头会贵，而在我们这个系统中，它只需要在中间件中加入一个用于动态识别报警的代码即可；

1. 人脸识别

在动态识别的基础上，可以加入人脸识别，当识别是用户时，则不会发出警报，但识别到未记录的人脸时，自动对焦并拍摄具有时间戳的照片；人脸识别也可以用于用户在对系统部件进行修改时的一个认证授权手段，确保是用户本人在修改程序；

1. 语音识别+智能助手+音频加密

在摄像头的基础上，还可支持录音，录制音频也会进行加密，它与图像组成一个文件，从而提高了监控系统的实用性；

还可以考虑加入智能助手，因为其实系统的中间件可以是微型电脑，电脑等可编程部件，那么在中间件配置允许的情况下，可加入智能助手来提高用户的体验度；

1. 日志记录并分析

日志可对异常的图像和音频进行记录，也可对入侵进行记录，并在一定程度上进行自动化分析，如果得到一定的危险等级就会自动报警，这就减少了因为误差等因素引起的报警，提高了准确度；同时，用户可以通过日志来对系统进行加固，来增强系统整体的安全性；

1. 技术亮点之加密算法

SM算法包括SM1（SCB2）、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法（ZUC)那等等。其中SM1、SM4、SM7、祖冲之密码（ZUC）是对称算法；SM2、SM9是非对称算法；SM3是哈希算法。而我们设计的摄像头系统中使用了SM2、SM3、SM4、祖冲之密码（ZUC），涵盖了我国商用密码算法的所有类型，并且我们密钥管理和生成规则上采用由用户主导的方式，用户可以自主设计生成规则，只需要修改对应的代码段即可；

从密码应用实践来看，我国商用密码算法在设计、实现方面均有优势，以SM算法为例，密钥替换攻击是目前多个数字签名算法不能抵御的攻击方法，SM2数字签名算法抵御密钥替换攻击方面存在可证明安全，SM2算法的性能与EC-SDSA等国际算法相当，但签名长度更短。SM3算法能够抵御差分分析且具有较强的扩散性，在硬件实现面积和性能上占优。SM4算法在设计上实现了资源重用，即密钥扩展过程和加密过程类似，实现时硬件资源占用较少，目前针对SM4的研究最多能分析32轮中的23轮，具有良好的安全强度。而ZUC算法，在利用现有分析方法对ZUC的整体安全性进行了评估之后,特别是线性区分攻击和差分攻击，得出一个结论：很大可能不存在一个可行的对于ZUC的线性区分攻击。

密钥存储和管理，当系统中未包含TPM安全芯片时，密钥存储在数据库中，安全性较低，但是因为存在于中间件中，不会存在被攻击篡改等事件；而如果系统中存在TPM安全芯片，那么密钥的存储和管理会受到TPM的保护，可以被攻击篡改的几率几乎为零；

引用

周春芳. LTE 国际标准序列密码算法ZUC 的安全性分析[D]. 北京. 中国科学院研究生院. 2011-11-01.