说明书

发明名称: 即时通信方法和系统

技术领域

[1] 本发明涉及通信技术领域，特别涉及一种即时通信方法和系统。

背景技术

[2] 随着通信技术的发展，即时通信软件的功能不断加强，不但可以通过即时通信软件发送文字、图片、表情等即时信息进行聊天，而且还可以通过即时通信软件发送音频、视频等即时信息进行聊天。

[3] 目前在通过音频、视频等即时信息进行聊天时，是直接将音频、视频等即时信息传输到对方，对方接收到音频、视频等后，直接显示音频、视频等。

[4] 然而，在实现本发明的过程中，发明人发现现有技术至少存在以下缺点：

[5] 现有方法直接将音频、视频等即时信息传输到对方，对方接收到音频、视频等即时信息后，直接显示音频、视频等即时信息，音频、视频等即时信息容易被任何第三方获取，音频、视频等即时信息的私密性得不到保护，安全性很低。

对发明的公开

技术问题

[6] 本发明 的目的在于提供一种即时信息的私密性得到保护，安全性好的 即时通信方法和系统 。

问题的解决方案

技术解决方案

[7] 为了解决现有技术的问题，本发明实施例提供了一种即时通信方法和系统。所述技术方案如下：

[8] 一方面，提供了一种即时通信方法，所述方法包括：

[9] 即时通信发送端获取即时通信接收端的指纹信息，并利用所述即时通信接收端的指纹信息对所述即时通信接收端进行身份认证；

[10] 当对所述即时通信接收端的身份认证成功后，所述即时通信发送端生成音视频信息，并对所述音视频信息进行加密，得到音视频加密信息；

[11] 所述即时通信发送端将所述音视频加密信息发送至所述即时通信接收端，使得所述即时通信接收端接收并对所述音视频加密信息进行解密，得到并显示所述音视频信息。

[12] 另一方面，提供了一种即时通信系统，所述系统包括：即时通信发送端；

[13] 所述即时通信发送端包括：

[14] 发端指纹传感器，用于获取即时通信接收端的指纹信息，并利用所述即时通信接收端的指纹信息对所述即时通信接收端进行身份认证；

[15] 音视频信息生成器，与所述发端指纹传感器相连接，用于当所述发端指纹传感器对所述即时通信接收端的身份认证成功后，生成音视频信息；

[16] 发端实时监控处理器，与所述音视频信息生成器相连接，用于当所述音视频信息生成器生成音视频信息后，对所述音视频信息进行加密，得到音视频加密信息；

[17] 音视频信息发送器，与所述发端实时监控处理器相连接，用于将所述发端实时监控处理器得到的音视频加密信息发送至所述即时通信接收端，使得所述即时通信接收端接收并对所述音视频加密信息进行解密，得到并显示所述音视频信息。

发明的有益效果

有益效果

[18] 本发明实施例提供的技术方案带来的有益效果是：

[19] 通过获取并利用即时通信接收端的指纹信息对即时通信接收端进行身份认证，并对音视频信息进行加密后再发送到即时通信接收端，使得经过身份认证的即时通信接收端，才能获取音视频信息，使得音频、视频等即时信息不容易被任何第三方获取，且获取的音视频信息是经过加密的，使得音频、视频等即时信息的私密性可以得到很好的保护，提高了安全性。

对附图的简要说明

附图说明

[20] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一

些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[21] 图1是本发明实施例一提供的一种即时通信方法流程图；

[22] 图2是本发明实施例二提供的一种即时通信方法流程图；

[23] 图3是本发明实施例三提供的一种即时通信系统结构示意图；

[24] 图4是本发明实施例三提供的另一种即时通信系统结构示意图；

[25] 图5是本发明实施例三提供的又一种即时通信系统结构示意图。

实施该发明的最佳实施例

本发明的最佳实施方式

[26] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

[27] 实施例一

[28] 本发明实施例提供了一种即时通信方法，参见图1，该方法包括：

[29] 101：即时通信发送端获取即时通信接收端的指纹信息，并利用即时通信接收端的指纹信息对即时通信接收端进行身份认证。

[30] 102：当对即时通信接收端的身份认证成功后，即时通信发送端生成音视频信息，并对音视频信息进行加密，得到音视频加密信息。

[31] 103：即时通信发送端将音视频加密信息发送至即时通信接收端，使得即时通信接收端接收并对音视频加密信息进行解密，得到并显示音视频信息。

[32] 进一步地，即时通信发送端获取即时通信接收端的指纹信息之前，还包括：

[33] 即时通信发送端向即时通信接收端发送交换密钥请求和即时通信发送端的指纹信息；

[34] 即时通信发送端接收即时通信接收端发送的确认交换密钥信息和即时通信接收端的指纹信息。

[35] 进一步地，即时通信发送端生成音视频信息，并对音视频信息进行加密，得到音视频加密信息，包括：

[36] 即时通信发送端获取启动音视频应用的指令，启动音视频应用、进行音视频操作、生成音视频信息；

[37] 即时通信发送端利用即时通信发送端的指纹信息对音视频信息进行加密，得到音视频加密信息。

[38] 进一步地，即时通信发送端利用即时通信发送端的指纹信息对音视频信息进行加密，得到音视频加密信息，包括：

[39] 即时通信发送端利用即时通信发送端的指纹信息对即时通信发送端生成的全部音视频信息进行加密，得到即时通信发送端全部的音视频加密信息；或

[40] 即时通信发送端利用即时通信发送端的指纹信息对即时通信发送端生成的部分音视频信息进行加密，得到即时通信发送端部分的音视频加密信息。

[41] 进一步地，即时通信接收端接收并对音视频加密信息进行解密之前，还包括：

[42] 即时通信接收端获取即时通信发送端的指纹信息，并利用即时通信发送端的指纹信息对即时通信发送端进行身份认证；

[43] 当对即时通信发送端的身份认证成功后，即时通信接收端执行接收并对音视频加密信息进行解密的步骤。

[44] 本发明实施例所述的即时通信方法，通过获取并利用即时通信接收端的指纹信息对即时通信接收端进行身份认证，并对音视频信息进行加密后再发送到即时通信接收端，使得经过身份认证的即时通信接收端，才能获取音视频信息，使得音频、视频等即时信息不容易被任何第三方获取，且获取的音视频信息是经过加密的，使得音频、视频等即时信息的私密性可以得到很好的保护，提高了安全性。

[45] 需要说明的是本发明实施例所述的即时通信方法可以应用于微博、QQ、MSN、skype、微信等各种即时通信软件中。并且，可以应用于一对一聊天中，也可以应用于群聊中，在群聊中没有即时通信发送端密钥的用户只能看到即时通信发送端发送的未加密部分的音视频信息，而不能看到加密部分的音视频信息。

发明实施例

本发明的实施方式

[46] 实施例二

[47] 本发明实施例提供了一种即时通信方法，参见图2，该方法包括：

[48] 201：即时通信发送端向即时通信接收端发送交换密钥请求和即时通信发送端

的指纹信息。

[49] 具体地，当即时通信发送端需要与即时通信接收端进行加密发送音视频信息时，可以向即时通信接收端发送交换密钥请求和即时通信发送端的指纹信息。

[50] 具体地，本发明实施例中指纹信息为密钥。

[51] 具体地，可以在即时通信发送端设置发端指纹传感器，通过发端指纹传感器提取与即时通信发送端对应的用户的指纹信息，得到即时通信发送端的指纹信息。并且，可以将即时通信发送端用户的指纹信息存储在即时通信发送端的存储器或服务器的存储器中。

[52] 202：即时通信接收端接收交换密钥请求和即时通信发送端的指纹信息，并确认是否与即时通信发送端交换密钥信息，如果确认交换，则执行203；否则，执210。

[53] 具体地，即时通信接收端可以将即时通信发送端的指纹信息存储在即时通信接收端的存储器或服务器的存储器中，当需要对即时通信发送端进行验证时，可以从存储的地方读取出相关信息进行验证。

[54] 203：即时通信接收端向即时通信发送端发送确认交换密钥信息和即时通信接收端的指纹信息。

[55] 具体地，可以在即时通信接收端设置发端指纹传感器，通过发端指纹传感器提取即时通信接收端用户的指纹信息。并且，可以将指纹信息存储在即时通信接收端的存储器或服务器的存储器中。

[56] 204：即时通信发送端接收即时通信接收端发送的确认交换密钥信息和即时通信接收端的指纹信息。

[57] 具体地，即时通信发送端可以将即时通信接收端的指纹信息存储在即时通信发送端的存储器或服务器的存储器中，当需要对即时通信接收端进行验证时，可以从存储的地方读取出相关信息进行验证。

[58] 205：即时通信接收端向即时通信发送端发送进行音视频通信的请求信息。即时通信发送端获取即时通信接收端的指纹信息，并利用即时通信接收端的指纹信息对即时通信接收端进行身份认证。

[59] 具体地，即时通信发送端查询存储指纹信息的地方，判断是否能够查询到与该

即时通信接收端相对应的指纹信息，如果能够查询到，则证明即时通信接收端的身份合法，对即时通信接收端的身份认证成功。

[60] 206：即时通信发送端判断对即时通信接收端的身份认证是否成功，如果成功则执行207；否则，结束。

[61] 207：即时通信发送端生成音视频信息，并对音视频信息进行加密，得到音视频加密信息。

[62] 其中，音视频信息包括录音或视频等信息。

[63] 具体地，对音视频信息进行加密时，可以是对全部的音视频信息进行加密，也可以是对用户选择的部分音视频信息进行加密，可以根据实际应用情况，选择需要加密的音视频信息，对此不做具体限定。

[64] 具体地，即时通信发送端生成音视频信息，并对音视频信息进行加密，得到音视频加密信息，包括：

[65] 即时通信发送端获取启动音视频应用的指令，启动音视频应用、进行音视频操作、生成音视频信息；

[66] 即时通信发送端利用即时通信发送端的指纹信息对音视频信息进行加密，得到音视频加密信息。

[67] 其中，即时通信发送端利用即时通信发送端的指纹信息对音视频信息进行加密，得到音视频加密信息，包括：

[68] 即时通信发送端利用即时通信发送端的指纹信息对即时通信发送端生成的全部音视频信息进行加密，得到即时通信发送端全部的音视频加密信息；或

[69] 即时通信发送端利用即时通信发送端的指纹信息对即时通信发送端生成的部分音视频信息进行加密，得到即时通信发送端部分的音视频加密信息。

[70] 208：即时通信发送端将音视频加密信息发送至即时通信接收端。

[71] 209：即时通信接收端接收并对音视频加密信息进行解密，得到并显示音视频信息，然后结束。

[72] 具体地，即时通信接收端接收并对音视频加密信息进行解密之前，还包括：

[73] 即时通信接收端获取即时通信发送端的指纹信息，并利用即时通信发送端的指纹信息对即时通信发送端进行身份认证；

[74] 当对即时通信发送端的身份认证成功后，即时通信接收端执行接收并对音视频加密信息进行解密的步骤。

[75] 210：即时通信接收端向即时通信发送端发送确认不交换密钥信息，然后结束。

[76] 本发明实施例所述的即时通信方法，通过获取并利用即时通信接收端的指纹信息对即时通信接收端进行身份认证，并对音视频信息进行加密后再发送到即时通信接收端，使得经过身份认证的即时通信接收端，才能获取音视频信息，使得音频、视频等即时信息不容易被任何第三方获取，且获取的音视频信息是经过加密的，使得音频、视频等即时信息的私密性可以得到很好的保护，提高了安全性。

[77] 实施例三

[78] 参见图3，本发明实施例提供了一种即时通信系统，该系统包括：即时通信发送端30；

[79] 即时通信发送端30包括：

[80] 发端指纹传感器301，用于获取即时通信接收端40的指纹信息，并利用即时通信接收端40的指纹信息对即时通信接收端40进行身份认证；

[81] 音视频信息生成器302，与发端指纹传感器301相连接，用于当发端指纹传感器301对即时通信接收端40的身份认证成功后，生成音视频信息；

[82] 发端实时监控处理器303，与音视频信息生成器302相连接，用于当音视频信息生成器302生成音视频信息后，对音视频信息进行加密，得到音视频加密信息；

[83] 音视频信息发送器304，与发端实时监控处理器303相连接，用于将发端实时监控处理器303得到的音视频加密信息发送至即时通信接收端40，使得即时通信接收端40接收并对音视频加密信息进行解密，得到并显示音视频信息。

[84] 进一步地，发端指纹传感器301，还用于提取与即时通信发送端30对应的用户的指纹信息，得到即时通信发送端30的指纹信息；

[85] 相应地，参见图4，即时通信发送端30还包括：

[86] 指纹信息发送器305，与发端指纹传感器301相连接，用于向即时通信接收端40发送交换密钥请求和发端指纹传感器301提取得到的即时通信发送端30的指纹信

息；

[87] 指纹信息接收器306，与即时通信发送端30的存储器或服务器的存储器相连接，用于接收即时通信接收端40发送的确认交换密钥信息和即时通信接收端40的指纹信息，并将即时通信接收端40的指纹信息存储在即时通信发送端30的存储器或服务器的存储器中。

[88] 其中，服务器是为即时通信发送端30、即时通信接收端40等之间的通信提供服务的一台或多台计算机等。

[89] 进一步地， 音视频信息生成器302，具体用于获取启动音视频应用的指令，启动音视频应用、进行音视频操作、生成音视频信息；

[90] 发端实时监控处理器303，具体用于利用即时通信发送端30的指纹信息对音视频信息进行加密，得到音视频加密信息。

[91] 进一步地，发端实时监控处理器303包括：

[92] 第一实时监控子处理器，与音视频信息生成器302相连接，用于利用即时通信发送端30的指纹信息对即时通信发送端30生成的全部音视频信息进行加密，得到即时通信发送端30全部的音视频加密信息；或

[93] 第二实时监控子处理器，与音视频信息生成器302相连接，用于利用即时通信发送端30的指纹信息对即时通信发送端30生成的部分音视频信息进行加密，得到即时通信发送端30部分的音视频加密信息。

[94] 进一步地，参见图5，该系统还包括：即时通信接收端40；

[95] 即时通信接收端40包括：

[96] 音视频信息接收器401，与音视频信息发送器304相连接，用于接收音视频信息发送器304发送的音视频加密信息；

[97] 接端指纹传感器402，与音视频信息接收器401相连接，用于在音视频信息接收器401接收到音视频信息发送器304发送的音视频加密信息后，获取即时通信发送端30的指纹信息，并利用即时通信发送端30的指纹信息对即时通信发送端30进行身份认证；

[98] 接端实时监控处理器403，与接端指纹传感器402相连接，用于当接端指纹传感器402对即时通信发送端30的身份认证成功后，对音视频加密信息进行解密，得

到并显示音视频信息。

[99] 需要说明的是，本发明实施例中各个设备之间相连接时，可以是通过有线方式、无线方式或其他方式进行连接，对此不做具体限定，可以根据实际应用状况进行设置。

[100] 本发明实施例所述的即时通信系统，通过获取并利用即时通信接收端的指纹信息对即时通信接收端进行身份认证，并对音视频信息进行加密后再发送到即时通信接收端，使得经过身份认证的即时通信接收端，才能获取音视频信息，使得音频、视频等即时信息不容易被任何第三方获取，且获取的音视频信息是经过加密的，使得音频、视频等即时信息的私密性可以得到很好的保护，提高了安全性。

[101] 需要说明的是：上述实施例提供的即时通信系统，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将系统的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的即时通信系统与即时通信方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[102] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[103] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成,所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[104] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权利要求书

[权利要求 1] 一种即时通信方法，其特征在于，所述方法包括：

即时通信发送端获取即时通信接收端的指纹信息，并利用所述即时通信接收端的指纹信息对所述即时通信接收端进行身份认证；

当对所述即时通信接收端的身份认证成功后，所述即时通信发送端生成音视频信息，并对所述音视频信息进行加密，得到音视频加密信息；

所述即时通信发送端将所述音视频加密信息发送至所述即时通信接收端，使得所述即时通信接收端接收并对所述音视频加密信息进行解密，得到并显示所述音视频信息。

[权利要求 2] 根据权利要求1所述的方法，其特征在于，即时通信发送端获取即时通信接收端的指纹信息之前，还包括：

所述即时通信发送端向所述即时通信接收端发送交换密钥请求和所述即时通信发送端的指纹信息；

所述即时通信发送端接收所述即时通信接收端发送的确认交换密钥信息和所述即时通信接收端的指纹信息。

[权利要求 3] 根据权利要求1所述的方法，其特征在于，所述即时通信发送端生成音视频信息，并对所述音视频信息进行加密，得到音视频加密信息，包括：

所述即时通信发送端获取启动音视频应用的指令，启动音视频应用、进行音视频操作、生成所述音视频信息；

所述即时通信发送端利用所述即时通信发送端的指纹信息对所述音视频信息进行加密，得到所述音视频加密信息。

[权利要求 4] 根据权利要求3所述的方法，其特征在于，所述即时通信发送端利用所述即时通信发送端的指纹信息对所述音视频信息进行加密，得到所述音视频加密信息，包括：

所述即时通信发送端利用所述即时通信发送端的指纹信息对所述即时通信发送端生成的全部音视频信息进行加密，得到所述即时

通信发送端全部的音视频加密信息；或

所述即时通信发送端利用所述即时通信发送端的指纹信息对所述即时通信发送端生成的部分音视频信息进行加密，得到所述即时通信发送端部分的音视频加密信息。

[权利要求 5] 根据权利要求1-4任一权利要求所述的方法，其特征在于，所述即时通信接收端接收并对所述音视频加密信息进行解密之前，还包括：

所述即时通信接收端获取所述即时通信发送端的指纹信息，并利用所述即时通信发送端的指纹信息对所述即时通信发送端进行身份认证；

当对所述即时通信发送端的身份认证成功后，所述即时通信接收端执行接收并对所述音视频加密信息进行解密的步骤。

[权利要求 6] 一种即时通信系统，其特征在于，所述系统包括：即时通信发送端；

所述即时通信发送端包括：

发端指纹传感器，用于获取即时通信接收端的指纹信息，并利用所述即时通信接收端的指纹信息对所述即时通信接收端进行身份认证；

音视频信息生成器，与所述发端指纹传感器相连接，用于当所述发端指纹传感器对所述即时通信接收端的身份认证成功后，生成音视频信息；

发端实时监控处理器，与所述音视频信息生成器相连接，用于当所述音视频信息生成器生成音视频信息后，对所述音视频信息进行加密，得到音视频加密信息；

音视频信息发送器，与所述发端实时监控处理器相连接，用于将所述发端实时监控处理器得到的音视频加密信息发送至所述即时通信接收端，使得所述即时通信接收端接收并对所述音视频加密信息进行解密，得到并显示所述音视频信息。

[权利要求 7] 根据权利要求6所述的系统，其特征在于，所述发端指纹传感器，还用于提取与所述即时通信发送端对应的用户的指纹信息，得到所述即时通信发送端的指纹信息；

相应地，所述即时通信发送端还包括：

指纹信息发送器，与所述发端指纹传感器相连接，用于向所述即时通信接收端发送交换密钥请求和所述发端指纹传感器提取得到的所述即时通信发送端的指纹信息；

指纹信息接收器，与所述即时通信发送端的存储器或服务器的存储器相连接，用于接收所述即时通信接收端发送的确认交换密钥信息和所述即时通信接收端的指纹信息，并将所述即时通信接收端的指纹信息存储在所述即时通信发送端的存储器或服务器的存储器中。

[权利要求 8] 根据权利要求6所述的系统，其特征在于，

所述音视频信息生成器，具体用于获取启动音视频应用的指令，启动音视频应用、进行音视频操作、生成所述音视频信息；

所述发端实时监控处理器，具体用于利用所述即时通信发送端的指纹信息对所述音视频信息进行加密，得到所述音视频加密信息。

[权利要求 9] 根据权利要求8所述的系统，其特征在于，所述发端实时监控处理器包括：

第一实时监控子处理器，与所述音视频信息生成器相连接，用于利用所述即时通信发送端的指纹信息对所述即时通信发送端生成的全部音视频信息进行加密，得到所述即时通信发送端全部的音视频加密信息；或

第二实时监控子处理器，与所述音视频信息生成器相连接，用于利用所述即时通信发送端的指纹信息对所述即时通信发送端生成的部分音视频信息进行加密，得到所述即时通信发送端部分的音视频加密信息。

[权利要求 10] 根据权利要求6-9任一权利要求所述的系统，其特征在于，所述系统还包括：所述即时通信接收端；

所述即时通信接收端包括：

音视频信息接收器，与所述音视频信息发送器相连接，用于接收所述音视频信息发送器发送的音视频加密信息；

接端指纹传感器，与所述音视频信息接收器相连接，用于在所述音视频信息接收器接收到所述音视频信息发送器发送的音视频加密信息后，获取所述即时通信发送端的指纹信息，并利用所述即时通信发送端的指纹信息对所述即时通信发送端进行身份认证；

接端实时监控处理器，与所述接端指纹传感器相连接,用于当所述接端指纹传感器对所述即时通信发送端的身份认证成功后，对所述音视频加密信息进行解密，得到并显示所述音视频信息。