



(19)中華民國智慧財產局

(12)發明說明書公告本

(11)證書號數：TW I684886 B

(45)公告日：中華民國 109 (2020) 年 02 月 11 日

(21)申請案號：106131723

(22)申請日：中華民國 106 (2017) 年 09 月 15 日

(51)Int. Cl. : G06F21/36 (2013.01)

(30)優先權：2016/11/24 中國大陸 201611053422.0

(71)申請人：香港商阿里巴巴集團服務有限公司 (香港地區) ALIBABA GROUP SERVICES LIMITED (HK)

香港

(72)發明人：董鵬贊 (CN)；孫娜 (CN)；江璇 (CN)；林述民 (CN)；李淵深 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW 201129049A

CN 1820288A

CN 105426744A

US 2010/0186083A1

審查人員：廖國智

申請專利範圍項數：58 項 圖式數：14 共 97 頁

(54)名稱

安全問題的生成以及身份驗證的方法及裝置

(57)摘要

本發明揭露了一種安全問題的生成以及身份驗證的方法及裝置，在生成安全問題時，首先，向終端發送安全問題的生成指令，以使得該終端返回在用戶操作下生成的基準圖片，其次，根據該基準圖片，確定若干與該基準圖片對應的混淆圖片，最後，根據該基準圖片以及各混淆圖片，生成安全問題，並當需要時使用該安全問題進行身份驗證。可見，由於該安全問題是基於該基準圖片生成的，而該基準圖片是在用戶的操作下生成的，所以提高了用戶在生成安全問題時的參與度，提高了用戶對該安全問題的記憶效果，提高了該安全問題的易用性，且無需採集分析用戶的行為資料，降低了生成成本，提高了身份驗證的效率。

指定代表圖：

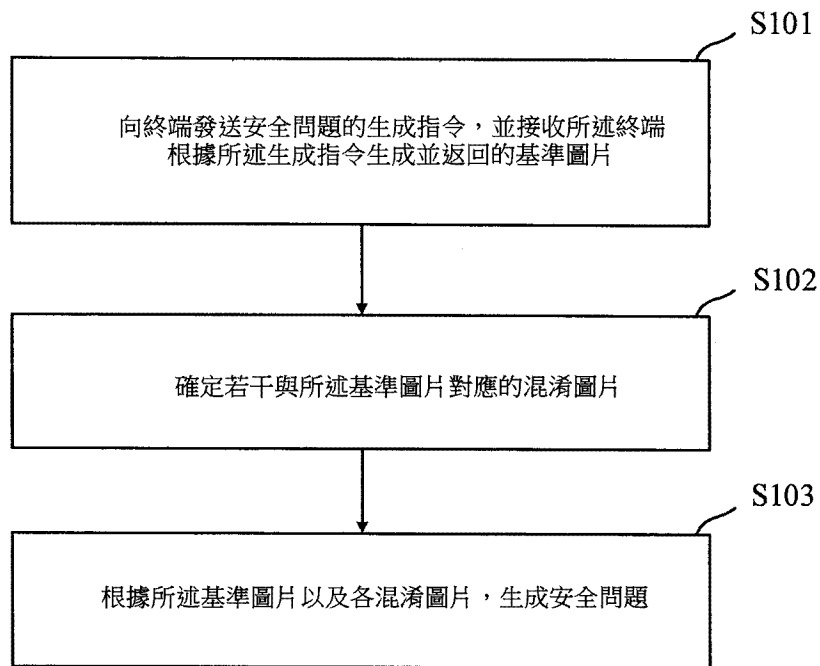


圖 1

【發明說明書】

【中文發明名稱】

安全問題的生成以及身份驗證的方法及裝置

【技術領域】

本發明關於資訊技術領域，尤其關於一種安全問題的生成以及身份驗證的方法及裝置。

【先前技術】

隨著資訊技術的發展，由於通過網路執行業務存在執行速度快、耗費資源少等優點，使得通過網路執行的業務越來越多，而為了保證通過網路執行業務的安全性，通常需要對業務發起方的身份驗證，於是，如何更準確、更方便、更快捷的進行身份驗證就成為了人們關注的重點問題之一。

在現有的身份驗證方法中，主要通過安全問題來對用戶的身份進行驗證，其中，安全問題以生成方式的不同主要可分為兩類：其一，通過引導用戶預先設置安全問題的題目以及答案，生成安全問題，第二，通過採集和分析用戶的歷史行為資料，生成用於身份驗證的安全問題。

對於第一類方式生成的安全問題，為了保證用戶預先設置的安全問題不會被輕易破解，所以在設置該安全問題時，通常會引導用戶設置一些不常用到的、事實內容的問題，例如，用戶的小學老師是誰、用戶的近親屬的生日日

期、喜歡的球隊名稱等等。由於該類不常用到的事實類問題，在用戶的日常生活之中出現的機率較低、出現的頻率較低，所以使得該類安全問題被破解的機率較低。

對於第二類方式生成的安全問題，由於該安全問題通過採集和分析用戶的歷史行為資料生成，所以該問題的題目以及答案與用戶的日常行為關係較為密切，例如，利用用戶的交易資訊、用戶的旅行資訊、用戶的好友關係生成安全問題等等。由於，每個用戶的行為具有獨特的個人特點，並且該問題也可關於只有用戶自身清楚的事實，所以既免去了用戶設置問題的操作，同時保證了該安全問題較難被破解。

但是，對於上述現有技術仍然存在以下缺點，對於通過第一類方式生成的安全問題，由於該安全問題屬於用戶不常用的問題，所以對用戶對該問題的正確答案的記憶提出了較高的要求，雖然可能使該安全問題難以破解，但是也使得用戶遺忘該問題的正確答案的機率大增，使得該安全問題的易用性受到影響。而對於通過第二類方式生成的安全問題，由於該安全問題需要基於用戶的歷史行為資料的採集和分析，所以通常需要採集用戶較多的歷史行為資料，以便分析和生成安全問題，若該用戶的歷史行為資料較少或者沒有，則難以生成安全問題，所以第二類方式生成的安全問題，對用戶的歷史行為資料的數量和品質都提出了要求，抬高了通過該方法生成安全問題的門檻，以及通過該方法生成安全問題的推廣門檻(即，應用範圍難以

擴大)。

可見，現有的身份驗證方式，由於生成安全問題的方式存在以上的缺陷，使得用於身份驗證的安全問題的易用性較低、生成要求較高，並且運行成本較高，導致身份驗證的效率較低。

【發明內容】

本發明實施例提供一種安全問題的生成方法及裝置，用於解決在採用現有的用於身份驗證的安全問題，易用性較低、生成要求較高，導致身份驗證成本較高，身份驗證效率低的問題。

本發明實施例提供一種身份驗證的方法及裝置，用於解決在採用現有的用於身份驗證的安全問題，易用性較低、生成要求較高，導致身份驗證成本較高，身份驗證效率低的問題。

本發明實施例提供一種安全問題的管理方法及裝置，用於解決在採用現有的用於身份驗證的安全問題，易用性較低、生成要求較高，導致身份驗證成本較高，身份驗證效率低的問題。

本發明實施例採用下述技術方案：

一種安全問題的生成方法，包括：

向終端發送安全問題的生成指令，並接收所述終端根據所述生成指令生成並返回的基準圖片；

確定若干與所述基準圖片對應的混淆圖片；

根據所述基準圖片以及各混淆圖片，生成安全問題。

一種安全問題的生成方法，包括：

接收伺服器發送的安全問題的生成指令；

監測用戶的操作，並根據監測到的所述操作生成基準圖片；

向所述伺服器返回所述基準圖片，以使得所述伺服器根據所述基準圖片生成安全問題。

一種身份驗證的方法，包括：

根據待驗證帳戶，確定用於生成與所述待驗證帳戶對應的安全問題的基準圖片；

根據所述基準圖片以及與所述基準圖片對應的各混淆圖片，生成安全問題；

向所述待驗證帳戶所在的終端發送所述安全問題；

接收所述終端返回的選擇結果，並根據所述選擇結果對所述待驗證帳戶進行身份驗證。

一種安全問題的管理方法，包括：

確定帳戶對應的各安全問題；

確定各安全問題分別對應的生成時間以及使用記錄；

根據各安全問題對應的生成時間以及使用記錄，確定各安全問題分別對應的有效期、優先順序以及冷卻期中的至少一種；

當對所述帳戶進行身份驗證時，根據各安全問題分別對應的有效期、冷卻期以及優先順序中的至少一種，從所述帳戶對應的各安全問題中，選擇用於身份驗證的安全問

題，並使用選擇的安全問題對應的安全問題對所述帳戶進行身份驗證。

一種安全問題的生成裝置，包括：

通訊模組，向終端發送安全問題的生成指令，並接收所述終端根據所述生成指令生成並返回的基準圖片；

確定模組，確定若干與所述基準圖片對應的混淆圖片；

生成模組，根據所述基準圖片以及各混淆圖片，生成安全問題。

一種安全問題的生成裝置，包括：

接收模組，接收伺服器發送的安全問題的生成指令；

監測生成模組，監測用戶的操作，並根據監測到的所述操作生成基準圖片；

發送生成模組，向所述伺服器返回所述基準圖片，以使得所述伺服器根據所述基準圖片生成安全問題。

一種身份驗證的裝置，包括：

確定模組，根據待驗證帳戶，確定用於生成與所述待驗證帳戶對應的安全問題的基準圖片；

生成模組，根據所述基準圖片以及與所述基準圖片對應的各混淆圖片，生成安全問題；

發送模組，向所述待驗證帳戶所在的終端發送所述安全問題；

驗證模組，接收所述終端返回的選擇結果，並根據所述選擇結果對所述待驗證帳戶進行身份驗證。

一種安全問題的管理裝置，包括：

第一確定模組，確定帳戶對應的各安全問題；

第二確定模組，確定各安全問題分別對應的生成時間以及使用記錄；

第三確定模組，根據各安全問題對應的生成時間以及使用記錄，確定各安全問題分別對應的有效期、優先順序以及冷卻期中的至少一種；

驗證選擇模組，當對所述帳戶進行身份驗證時，根據各安全問題分別對應的有效期、冷卻期以及優先順序中的至少一種，從所述帳戶對應的各安全問題中，選擇用於身份驗證的安全問題對所述帳戶進行身份驗證。

本發明實施例採用的上述至少一個技術方案能夠達到以下有益效果：

在生成安全問題時，首先，向終端發送安全問題的生成指令，以使得該終端監測在用戶的操作下生成的基準圖片，並將該基準圖片返回，其次，根據該基準圖片，確定若干與該基準圖片對應的混淆圖片，最後，根據該基準圖片以及各混淆圖片，生成安全問題，並當需要時使用該安全問題進行身份驗證。可見，由於該安全問題是基於該基準圖片生成的，而該基準圖片是在用戶的操作下生成的，所以提高了用戶在生成安全問題時的參與度，提高了用戶對該安全問題的記憶效果，提高了該安全問題的易用性，且無需採集分析用戶的行為資料，降低了生成成本，提高了身份驗證的效率。

【圖式簡單說明】

此處所說明的附圖用來提供對本發明的進一步理解，構成本發明的一部分，本發明的示意性實施例及其說明用於解釋本發明，並不構成對本發明的不當限定。在附圖中：

圖1為本發明實施例提供的一種安全問題的生成過程；

圖2為本發明實施例提供的本發明實施例還提供該基準圖片X的取值範圍的示意圖；

圖3是本發明實施例提供的發送安全問題以及發送保存詢問資訊的過程示意圖；

圖4a-圖4b為本發明實施例提供的安全問題的標識的優先順序隨時間變化的示意圖；

圖5為本發明實施例提供的在向量空間中該距離範圍、各待選圖片的向量以及該基準圖片的向量的對應關係

圖6為本發明實施例提供的一種安全問題的生成過程；

圖7為本發明實施例提供的基準圖片的設置介面示意圖；

圖8為本發明實施例提供的安全問題生成的詳細流程圖；

圖9為本發明實施例提供的一種身份驗證方法；

圖10為本發明實施例提供的一種安全問題的管理方

法；

圖 11 為本發明實施例提供的一種安全問題的生成裝置的結構示意圖；

圖 12 為本發明實施例提供的另一種安全問題的生成裝置的結構示意圖；

圖 13 為本發明實施例提供的一種身份驗證的裝置的結構示意圖；

圖 14 為本發明實施例提供的一種安全問題的管理裝置的結構示意圖。

【實施方式】

為使本發明的目的、技術方案和優點更加清楚，下面將結合本發明具體實施例及相應的附圖對本發明技術方案進行清楚、完整地描述。顯然，所描述的實施例僅是本發明一部分實施例，而不是全部的實施例。基於本發明中的實施例，本領域普通技術人員在沒有做出進步性勞動前提下所獲得的所有其他實施例，都屬於本發明保護的範圍。

以下結合附圖，詳細說明本發明各實施例提供的技術方案。

圖 1 為本發明實施例提供的一種安全問題的生成過程，具體包括以下步驟：

S101：向終端發送安全問題的生成指令，並接收所述終端根據所述生成指令生成並返回的基準圖片。

通常由於身份驗證過程所需的安全問題，用於對使用

業務(或者，發起業務請求)的用戶身份進行驗證，所以如何生成安全問題以及生成哪些種類的安全問題，通常也是由提供業務服務的一方決定的(即，不是由用戶決定的)，於是，一般情況下在生成安全問題時，可由提供業務服務一方的伺服器向使用業務一方的終端發送安全問題的生成指令(即，由伺服器向終端發送安全問題的生成指令)，以使得該操作該終端的用戶可以在該生成指令的引導下，完成安全問題的設置，以便在有身份驗證的需要時，可以通過該安全問題進行身份驗證。同理，在本發明中，可由伺服器向終端發送安全問題的生成指令。

另外，需要說明的是，由於通常用戶需要通過帳戶執行業務，不同的帳戶可以對應於不同的用戶，而身份驗證是對用戶的身份進行驗證的，所以該伺服器可通過帳戶發送該生成指令至該終端。

其中，該伺服器可採用多種方式，確定向哪一個帳戶所在的終端發送安全問題，例如，確定上一時刻註冊完成的各帳戶，並通過各帳戶向各終端發送安全問題的生成指令，或者輪詢各註冊完成的帳戶，並確定沒有安全問題的各帳戶，並通過各帳戶向各終端發送安全問題的生成指令，等等，本發明對於如何發起安全問題的生成指令的方式並不做限定。

進一步地，與現有技術相同，該伺服器在發送安全問題的生成指令之前，還可確定該終端上登錄的該帳戶在當前登錄有效期內已通過了身份驗證，以保證後續生成的安

全問題的有效性，當然，本發明不限定具體採用什麼方法確定該終端上登錄的該帳戶在當前登錄有效期內已通過了身份驗證，該伺服器可根據實際應用的需要對該終端上登錄的該帳戶進行身份驗證，並且，在該帳戶的身份驗證通過時，繼續後續的操作。

更進一步地，在本發明實施例中，該生成指令可用於使該終端根據該生成指令生成該基準圖片，並將該基準圖片返回該伺服器，當然，為了使該伺服器可以確定該基準圖片對應的帳號，所述該生成指令還可以使該終端將該帳戶的標識以及該基準圖片返回該伺服器，於是，該伺服器還可以接收該終端根據該生成指令生成並返回的該基準圖片以及該帳戶的標識。

具體的，該生成指令中可以包含文字、圖片、音訊以及視頻等資訊，用以在該終端上顯示，並引導使用該終端的用戶執行操作，在該終端上生成該基準圖片。其中，該操作可以包括：手勢操作、語音操作等等，該操作具體可根據實際應用的需求確定，只要該終端可以在用戶的操作下生成該基準圖片即可，例如，該基準圖片可以是用戶通過手勢操作繪畫出的一張圖片，可以是用戶通過手勢操作使用該終端的攝像頭拍攝的一張圖片等等，可以是用戶通過語音使該終端拍攝一張圖片等等，即，該基準圖片可通過多種方式生成。

需要說明的是，在本發明實施例中，該終端可以是手機、平板電腦等終端，該伺服器可以是單獨的一台設備，

可以是有多台設備組成的系統，即，分散式伺服器，本發明對此不做具體限定。

S102：確定若干與所述基準圖片對應的混淆圖片。

在本發明實施例中，由於在步驟**S101**中該終端返回了該基準圖片，所以該伺服器可以根據該基準圖片，確定對應的混淆圖片，以便後續基於該基準圖片以及混淆圖片生成該安全問題。

由於，該基準圖片的生成過程是在用戶的參與下完成的，所以該用戶對該基準圖片的特徵以及細節通常是最為清楚的，於是在本發明中，該伺服器可基於該基準圖片作為該安全問題的正確選項，生成該安全問題。同時，在生成該安全問題時還需要一定數量錯誤選項，用於在該安全問題中作為混淆選項，以提高該安全問題的保密性，所以該伺服器還可確定與該基準圖片相似的混淆圖片，並以該混淆圖片作為錯誤選項，並且，該伺服器確定的該混淆圖片也不能與該基準圖片過於相似，使得生成該基準圖片的用戶也無法分辨出該基準圖片與混淆圖片的區別。

於是，在本發明中，該伺服器可先確定該基準圖片的特徵值，以便根據該特徵值篩選出合適的混淆圖片，於是該伺服器可以確定該基準圖片的特徵值。

具體的，在本發明實施例中，該伺服器可以根據預設的特徵提取模型，確定該基準圖片的特徵值，其中，特徵提取模型可以有多個，並且可包含：顏色特徵模型、圖形特徵模型以及複雜度特徵模型中的至少一種。

其中，該色彩模型可以是色調、飽和度、明度(Hue、Saturation、Value，HSV)模型，通過該色彩模型可以確定該基準圖片的每一個像素點的色調值、飽和度值以及明度值，並以該基準圖片的每一個像素點的色調值對應的矩陣作為該基準圖片的特徵值、以該基準圖片的每一個像素點的飽和度值對應的矩陣作為該基準圖片的特徵值以及以該基準圖片的每一個像素點的色調值對應的矩陣作為該基準圖片的特徵值，可以是顏色矩對應的該基準圖片的顏色一階矩、顏色二階矩和顏色三階矩，並將該顏色矩作為該基準圖片的顏色特徵值等等。

該形狀特徵值模型，可以是利用邊界特徵法計算確定的該基準圖片的形狀特徵值，可以是通過傅裡葉形狀描述符(Fourier Shape Descriptors)確定的該基準圖片的形狀特徵值，可以是利用形狀不變矩法，以任一形狀區域的矩作為形狀描述參數確定的該基準圖片的形狀特徵值等等。

該複雜度特徵模型，可以是利用該基準圖片的灰階長條圖中，各灰階在該基準圖片中出現頻率作為該基準圖片的複雜度特徵值，可以是利用該基準圖片的灰階長條圖的灰階共生矩陣，生成的該基準圖片的紋理特徵值，作為該基準圖片的複雜度特徵值等等。

也就是說，在本發明中，可以使用現有技術中的對圖像特徵提取的任何模型、方法等，確定該基準圖片的多種特徵值，具體的該圖像特徵提取的方式可採用與現有技術相同的方式來確定該基準圖片的特徵值，並且該基準圖片

對應的特徵值至少有一個即可，即，本發明並不限定具體使用何種方式確定該基準圖片的特徵值。

進一步地，當該伺服器確定了該基準圖片的特徵值之後，便可根據該特徵值確定與所述基準圖片對應的各混淆圖片。

如前所述，由於各混淆圖片的作用是：減少除了使用該終端生成該基準圖片的用戶以外的其他用戶，在面對後續生成的該安全問題時，選擇出該基準圖片的機率，所以各混淆圖片的特徵值可與該基準圖片的特徵值相近，以起到混淆的作用。另一態樣，若各混淆圖片與該基準圖片過於相似(即，特徵值過於相近)時，也會增加使用該終端生成該基準圖片的用戶無法分辨該基準圖片與各混淆圖片的機率，所以在本發明中，各混淆圖片的特徵值可與該基準圖片的特徵值也可存在一定的差異。

具體的，確定的該基準圖片的特徵值，該伺服器可以預先配置的取值策略，確定該基準圖片對應的取值範圍，並根據該取值範圍，從已儲存的待選圖片池中，確定落入該取值範圍內的待選圖片，作為與該基準圖片對應的混淆圖片，其中，該待選圖片池由各待選圖片組成。

第一步，該伺服器在確定該基準圖片對應的取值範圍時，為了避免確定的該混淆圖片與該基準圖片過於相似或者過於不相似，該伺服器確定的該取值範圍的最大值與該基準圖片的特徵值的差值不大於預設的最大值，且確定的該取值範圍的最小值與該基準圖片的特徵值的差值不小於

預設的最小值，並且確定的該特徵值不在該取值範圍內。即，以該特徵值為基準，在該特徵值的兩側確定該特徵值的取值範圍，使得該取值範圍與該特徵值即不過於相近，差異也不過大。需要說明的是，具體採用何種方法確定該取值策略本發明不作限定，如，根據經驗確定、根據機器學習的方法確定等等。

進一步地，由於對於不同的特徵值，該伺服器可以採用不同的取值策略，於是，在該伺服器中儲存的取值策略可根據針對的特徵值不同而不同，如表1所示。

特徵值標識	特徵值區間	取值策略
特徵值 A	0~100	±12~15
特徵值 B	0~255	+90~150
特徵值 C	-10~150	±110~120

表 1

其中，該特徵值區間表示該特徵值的可取的最大值以及最小值(例如，在 RGB 色彩空間中，每個顏色的取值區間為 0~255，也就是最大值可取 255 最小值可取 0)，該取值策略表示以該特徵值的數值為基準對應的取值範圍。需要說明的是，表 1 中所示“±”符號表示該特徵值對應的取值區間為增加量以及減少量，同理“+”符號表示該特徵值對應的取值區間為增加量，“-”符號表示該特徵值對應的取值區間為減少量。

例如，假設對於基準圖片 X，確定該基準圖片 X 的特徵值 A 為 35、特徵值 B 為 20、特徵值 C 為 16，則該基準圖片

X根據表1所示的取值策略，確定的取值範圍可如表2所示。

特徵值標識	特徵值(即，基準)	取值範圍
特徵值A	35	47~50&20~23
特徵值B	20	110~170
特徵值C	16	116~136&不存在

表2

其中，可見對於特徵值A和特徵值C對應的取值範圍均有兩組，即符號“±”所表示的增加量以及減少量，而特徵值B對應的取值範圍為增加量，所以該特徵值B對應的取值範圍只有一個，即“110~170”。並且，由於特徵值C的特徵值區間為“-10~150”，所以在本發明中特徵值C在取值策略“±110~120”下僅對應有一個增加量對應的取值範圍在該特徵值區間內，即“116~136”，減少量對應的取值範圍已經超出該特徵值C的特徵值區間，即“-104~-94”不在特徵值區間“-10~150”的範圍內，所以“不存在”。

為方便理解，本發明實施例還提供該基準圖片X的取值範圍的示意圖，如圖2所示。其中，該特徵值A、B、C分別以三段線段表示，該三段線段的端點即表示該特徵值A、B、C分別可取的最大值以及最小值，該基準圖片X的特徵值，以在該三段線段上的點表示，該基準圖片X的取值範圍以在該三段線段上的粗線表示，可見，該基準圖片X的取值範圍沒有包含該基準圖片X的特徵值。

第二步，該伺服器在確定了該基準圖片對應的取值範

圍之後，還可根據該取值範圍，從已儲存的待選圖片池中，確定特徵值落入該取值範圍之內的待選圖片，作為與該基準圖片對應的混淆圖片。

具體的，該伺服器中可預先儲存由若干待選圖片組成的待選圖片池，以便該伺服器可以根據該取值範圍，從該待選圖片池中確定落入該取值範圍內的待選圖片，並後續生成該安全問題。其中，該待選圖片池中的各待選圖片可由工作人員人工添加進該待選圖片池中，也可由該伺服器通過網路從各種資料庫中獲取，本發明對獲取該待選圖片池中的各待選圖片的過程不作具體限定。

並且，針對該待選圖片池中的每一個待選圖片，由於確定該待選圖片是否可作為與該基準圖片對應的混淆圖片，是根據該待選圖片的特徵值是否落入該基準圖片的取值範圍內確定的，所以為了節省該伺服器確定與基準圖片對應的混淆圖片時耗費的時間，該伺服器可在儲存該待選圖片之前，便預先確定該待選圖片的特徵值，並儲存該待選圖片以及該待選圖片的特徵值(即，該待選圖片池中的各待選圖片的特徵值可預先確定)，以便當確定該基準圖片對應的該混淆圖片時，可以根據已儲存的各待選圖片的特徵值，確定落入該基準圖片的取值範圍內的待選圖片作為混淆圖片。當然，本發明並不限定採用上述方法確定各待選圖片的特徵值，何時以及如何確定該待選圖片池中的各待選圖片的特徵值也可採用其他方式。

另外，若該伺服器沒確定任何一個待選圖片落入該取

值範圍，則可返回錯誤資訊，並向該終端重新發送如步驟S101中所述的該生成指令，直至確定至少一個混淆圖片為止。

S103：根據所述基準圖片以及各混淆圖片，生成安全問題。

在本發明實施例中，該伺服器在確定了該基準圖片以及與該基準圖片對應的各混淆圖片之後，便可以生成該安全問題。

具體的，首先，由於該伺服器在步驟S102中確定的與該基準圖片對應的各混淆圖片的數量無法預先確定，所以該伺服器可能確定出大量與該基準圖片對應的混淆圖片，而在生成該安全問題時，若將所有的混淆圖片與該基準圖片全部作為該安全問題的答題選項，則可能造成選項過多，以至於用戶難以回答該安全問題(例如，該安全問題的答題選項有50個，則用戶瀏覽各選項都需要耗費大量時間，從50個答題選項中確定正確答案就更困難了)，所以在本發明中，該伺服器可以先從與該基準圖片對應的各混淆圖片中，確定指定數量的混淆圖片。其中，該指定數量可由工作人員根據實際應用時的需要進行設置，或者根據該基準圖片對應的混淆圖片的數量確定，具體的該指定數量如何確定本發明不做具體限定。

其次，該伺服器可將該基準圖片以及指定數量的各混淆圖片，作為答題選項，生成該安全問題，即，以該基準圖片作為正確的答題選項，將指定數量的各混淆圖片作為

錯誤的答題選項，生成選擇題形式的安全問題。

進一步地，由於在步驟S101中所述的，該安全問題可用於對該帳戶進行身份驗證，所以該伺服器在生成該安全問題時，還可生成該安全問題的標識，並將該安全問題、該安全問題的標識以及該安全問題與該安全問題的標識的對應關係保存，以便後續需要使用該安全問題時，可根據該安全問題的標識確定該安全問題，並使用該安全問題(如，向待驗證帳戶發送該安全問題)。

更進一步地，該伺服器在保存該安全問題時，還可以保存該基準圖片、該基準圖片與各混淆圖片的對應關係，並在確定需要使用該安全問題時，通過保存的該基準圖片、該基準圖片與各混淆圖片的對應關係，確定該安全問題。也就是說，在本發明中，該伺服器在通過步驟S103生成該安全問題之後，由於該安全問題並不一定是立刻就要使用的，所以在保存該安全問題時，該伺服器也可僅保存生成該安全問題的基礎(即，該基準圖片、該基準圖片與各混淆圖片的對應關係)，並在需要使用該安全問題時，再根據該基準圖片、該基準圖片與各混淆圖片的對應關係，將該安全問題“組合”起來。具體在實際應用過程採用那種方式，本發明並不做具體限定，只要該安全問題是由該基準圖片以及確定的混淆圖片分別作為答題選項的安全問題即可。

通過如圖1所示的安全問題的生成方法，該伺服器在生成該安全問題時，是基於的是用戶在該終端上操作而生

成的基準圖片，由於該基準圖片生成的時間可以是任一時刻，所以增加了他人預謀盜取該基準圖片的成本，並且該基準圖片具體是什麼內容也僅有該用戶知曉，他人即使能瞭解該用戶的生活習慣、取得該用戶的個人資訊，也難以確定該基準圖片的具體內容，所以該基準圖片的安全性較高。同時，由於該基準圖片是在用戶的操作下生成的，增加了用戶對該安全問題設置的參與度，所以該用戶對於該基準圖片較為瞭解，增加了該用戶對該基準圖片的記憶力，減少了用戶遺忘該基準圖片的機率。可見，本發明實施例提供的方法，可以生成利於用戶記憶，安全性較高的安全問題，並且，由於生成安全問題時無需借助用戶的歷史行為資料，所以也提高了安全問題的易用性，降低了運行成本，提高了身份驗證的效率。

另外，在本發明中步驟 S102 該伺服器確定各混淆圖片的過程中，由於針對步驟 S101 中該終端生成的該基準圖片，該伺服器確定的混淆圖片越多，生成的安全問題的答題選項的自由度就越高(如，假設安全問題有 3 個選項，則除去該基準圖片對應的答題選項以外，還需要兩張混淆圖片分別對應的答題選項，若確定的與該基準圖片對應的混淆圖片只有兩張，則該安全問題的答題選項就只能固定的，而若確定的混淆圖片有兩張以上，則該安全問題的答題選項的可以有更多的變化，也就是說各混淆圖片越多，則在生成該安全問題時，答題選項的選擇自由度就越大)。並且，由於生成該安全問題的答題選項的自由度越

高，該安全問題被重複使用時，重複出現同樣的答題選項的機率就越小，則該安全問題的安全性也就越高，所以在步驟 S102 中，該伺服器還可根據確定的該混淆圖片的數量，確定是否繼續執行後續的步驟。

具體的，在該伺服器中，還可預先配置有混淆圖片的數量閾值，在步驟 S102 中當該伺服器確定的該基準圖片對應的混淆圖片的數量不小於預設的混淆圖片數量閾值時，該伺服器可確定繼續執行後續步驟 S103，當確定圖片對應的混淆圖片的數量小於預設的混淆圖片數量閾值時，該伺服器可確定執行步驟 S101 重新發送該生成指令至該終端，並且其中還可以攜帶有提示資訊，如，文字資訊：“生成的安全問題選項過少，請重新繪製/拍攝一張圖片”。

進一步地，在本發明中，步驟 S102 中確定的該基準圖片的特徵值，可視為執行後續步驟 S103 的基礎，而該基準圖片的圖片品質決定了提取的該基準圖片的特徵值可以唯一表示該基準圖片的機率(即，該基準圖片的特徵值可否準確的表示該基準圖片)，當該基準圖片的圖片品質越高，則該基準圖片的特徵值唯一表示該基準圖片的機率就越高，若該基準圖片的圖片品質較低，則確定的該基準圖片的特徵值可同時表示多個圖片的機率就較高，而唯一表示該基準圖片的機率較低，使得後續確定的各混淆圖片與該基準圖片之間存在較大差異的可能性增加，使得各混淆圖片用於混淆正確選項的作用下降，導致生成的安全問題的品質下降。

所以在本發明中，為了保證後續生成的該安全問題的品質，該伺服器在生成該安全問題之前，還可以判斷該基準圖片是否滿足預設的條件，其中，該條件包括以下至少一種：該基準圖片的像素數量不小於預設的像素數量、該基準圖片的儲存佔用空間不小於預設的儲存佔用空間、該基準圖片的內容分類不屬於預設的分類。

其中，對於該基準圖片的像素數量以及儲存佔用空間的預設條件，可以保證該基準圖片的圖片品質，即，保證該基準圖片足夠大、足夠清晰的圖片，以便提取較為準確的特徵值，而對該基準圖片的內容分類的預設條件，則可從該基準圖片的內容上排除該基準圖片是色情圖片、政治敏感圖片、廣告圖片等攜帶不良資訊的圖片。其中，該預設的像素數量、該預設的儲存佔用空間以及該預設的分類，均可由工作人員根據實際應用的需要設置。

需要說明的是，該基準圖片的內容分類在本發明中，採用“黑名單”的方式，排除該基準圖片是不良資訊的可能，即該預設條件是：所述基準圖片的內容分類不屬於預設的分類。但是，該伺服器也可採用“白名單”的方式，確定該基準圖片不包含不良資訊，則該預設條件也可以是：所述基準圖片的內容分類屬於預設的分類。

另外，由於在確定圖片品質時，該基準圖片的色彩資訊也關係到該基準圖片的像素數量以及儲存佔用空間，例如，一張彩色圖片與一張黑白圖片，在具有相同的像素數量時，分別對應的儲存佔用空間是不同的，但是可能該彩

色圖片與該黑白圖片都具有同樣的清晰度，所以在本發明中，該伺服器可針對彩色圖片以及黑白圖片，分別預設兩個儲存佔用空間的條件，即，彩色圖片儲存佔用空間以及黑白圖片儲存佔用空間，並在確定該基準圖片是否滿足預設的條件之前，該伺服器先根據該基準圖片的色彩資訊，判斷該基準圖片是彩色圖片還是黑白圖片，並根據判斷結果，確定該基準圖片的預設條件。

或者，該伺服器在確定該基準圖片的儲存佔用空間時，可根據該基準圖片的色彩資訊對該基準圖片的儲存佔用空間進行補正，具體方法，可採用以人工經驗確定補正係數，對黑白圖片的儲存佔用空間進行補正，當然，本發明也不限制採用其他方法就該基準圖片的儲存佔用空間進行補正，對此也不做具體限定。

進一步地，由於在現有技術中存在多種對圖片的內容分類進行篩查，以減少網路上不良資訊的方法，而在本發明中，該預設條件：該基準圖片的內容分類不屬於預設的分類，也可視為一種對圖片內容分類進行篩查的過程，所以在本發明中，也可採用與現有技術相同的方法確定該基準圖片的內容分類不屬於預設的分類，如，通過機器學習生成的模型，判斷該基準圖片的內容是否滿足預設的條件，或者通過人工篩查的方式判斷該基準圖片的內容是否滿足預設的條件，或者多種方法相結合的方式，本發明不做具體限定。

當然，若該伺服器確定該基準圖片不滿足預設條件，

則該伺服器還可向該終端發送提示資訊並重新執行步驟 S101，直至該終端返回的該基準圖片滿足預設條件為止。其中，該提示資訊可以包含將該基準圖片不滿足的預設條件，例如，當該基準圖片的像素數量不滿足要求時，該提示資訊可包含“您設置的圖片的像素數量不滿足要求，請提高設置圖片的品質，並重新發送”。

需要說明的是，在本發明中該伺服器可在生成該安全問題之前，確定該基準圖片滿足預設條件，但是考慮到該伺服器執行步驟 S102 會耗費一定的資源，所以為了減少該伺服器的運行壓力、減少資源耗費以及減少時間浪費，在本發明中，該伺服器也可以在步驟 S101 中接收到該基準圖片時，對該基準圖片的是否滿足預設的條件進行判斷，或者該伺服器也可以在步驟 S102 中對該基準圖片的是否滿足預設的條件進行判斷，具體的該伺服器在何時判斷該基準圖片是否滿足預設的條件本發明不做具體限定，可根據實際應用的需要確定，只要在生成該安全問題之前進行即可。

進一步地，由於在步驟 S101 中該終端生成的該基準圖片，有可能是該終端的感測器採集的圖像(如，用戶使用該終端的攝像頭拍攝的照片)，所以該基準圖片存在暴露該用戶個人隱私的資訊的可能性(如，用戶拍攝的是該用戶的汽車、住房等等，則車牌號、門牌號存在洩漏該用戶的個人隱私的可能)，所以為了減少由於該基準圖片作為安全問題的答題選項，造成用戶的隱私洩露的機率，並更

好的保護用戶的個人隱私，在本發明實施例中生成該安全問題之前，該伺服器還可以對該基準圖片進行模糊處理，作為該基準圖片的副本，並在步驟S103中將該基準圖片的副本以及各混淆圖片作為答題選項，生成該安全問題。

具體的，該伺服器可根據預設的顆粒度數值以及模糊強度數值，將所述基準圖片進行模糊處理，並將進行模糊處理的圖片作為所述基準圖片的副本，其中，該顆粒度數值以及該模糊強度數值可根據實際應用的需要由工作人員設置。

另外，由於生成該安全問題時，該基準圖片的副本是經過模糊處理的該基準圖片，所以該基準圖片的副本從清晰度以及圖片品質上可能與各混淆圖片存在差異，這就使得該伺服器在以該基準圖片的副本和各混淆圖片作為答題選項生成該安全問題的時，該基準圖片與各混淆圖片的差異過大，使該基準圖片的副本在作為答題選項時，在該安全問題的各答題選項中顯得過於突兀，使得該安全問題的安全性大大降低。

所以在本發明中，該伺服器在生成該安全問題之前，還可將確定的與該基準圖片對應的各混淆圖片進行模糊處理，並將該基準圖片的副本以及經過模糊處理的各混淆圖片作為答題選項，生成該安全問題。其中，對各混淆圖片進行模糊處理的過程，可與對該基準圖片進行模糊處理的過程一致，並且，進行模糊處理時所使用的顆粒度數值以及該模糊強度數值也可一致，以使得該安全問題的各答題

選項的模糊程度一致，

需要說明的是，若該安全問題在生成時，採用的該基準圖片作為答題選項，則各混淆圖片無需進行模糊處理，若該安全問題在生成時，採用的是該基準圖片的副本作為答題選項，則各混淆圖片可進行模糊處理。

當然，當需要對各混淆圖片進行模糊處理時，該伺服器也可預先對各混淆圖片進行模糊處理，如，確定與該基準圖片對應的各混淆圖片時，或者該伺服器在儲存各待選圖片時，便對各待選圖片進行模糊處理。當然，由於圖片進行模糊處理後提取的特徵值的準確度較低，所以在對各待選圖片進行模糊處理之前，該伺服器可先提取各待選圖片的特徵值，針對每一個待選圖片，對該待選圖片進行模糊處理後，將該待選圖片、該待選圖片的特徵值、經過模糊處理後的該待選圖片保存在本地，並記錄該待選圖片、該待選圖片的特徵值、經過模糊處理後的該待選圖片的對應關係。則該伺服器在確定與該基準圖片對應的各混淆圖片時，可從待選圖片池中選擇經過模糊處理的待選圖片，作為與該基準圖片對應的各混淆圖片。當然，本發明並不具體的限定何時對各混淆圖片進行模糊處理。

更進一步地，由於通常該終端生成的圖片均會自動保存在該終端本地，所以該基準圖片也可被該終端保存在該終端本地，這就使得生成的該安全問題存在一定的安全隱患(如，不法分子通過駭客軟體入侵該終端，並獲取了該終端中儲存的該基準圖片，則該不法分子破解該安全問題

的機率將會提高)，於是，為了提高生成的該安全問題的安全性，在本發明中，該伺服器在生成安全問題之前，還可以向該終端發送刪除該基準圖片的指令，並在本地保存該基準圖片、該基準圖片的副本。當然，該伺服器可以在接收到該基準圖片後，生成該安全問題之前的任一時刻，發送刪除該基準圖片的指令，本發明對此不做限定。

另外，為了加深用戶對該安全問題的理解以及對該基準圖片的記憶，所以在本發明中，該伺服器還可以向該終端發送該安全問題，以使得該用戶試答該安全問題，並將安全問題的答題結果返回該終端，說明該用戶對該安全問題的理解和記憶，並且，該伺服器還可向該終端發送是否保存所述安全問題的詢問資訊，並根據該終端返回的結果，保存或者刪除該安全問題。

具體的，首先，該伺服器可向該終端發送生成的該安全問題，其次，根據該終端返回的對該安全問題的答題結果，確定該終端的身份驗證結果，之後，將該身份驗證結果以及是否保存該安全問題的詢問資訊發送至該終端，最後，當該終端返回保存該安全問題的資訊時，保存該安全問題，當該終端返回不保存該安全問題的資訊時，刪除該安全問題，詳細過程可如圖3所示。

圖3為本發明實施例提供的伺服器發送安全問題以及保存詢問資訊的過程示意圖。

S1031：向該終端發送生成的該安全問題。

S1032：根據該終端返回的對該安全問題的答題結

果，確定該終端的身份驗證結果。

S1033：將該身份驗證結果以及是否保存該安全問題的詢問資訊，發送至該終端。

S1034：當該終端返回保存該安全問題的資訊時，保存該安全問題。

S1035：當該終端返回不保存該安全問題的資訊時，刪除該安全問題。

通過如圖3所示的過程，可以使用戶加深對該基準圖片的記憶的同時，使用戶可以對是否使用該基準圖片生成該安全問題進行選擇，提高了用戶的體驗。

另外，如圖3中所述的該安全問題的任一答題選項是該基準圖片的副本時(而不是該基準圖片時)，則當該用戶選擇的答題結果不是該基準圖片的副本對應的答題選項時，該伺服器還可以向該終端返回正確的答題選項，即，該基準圖片的副本，以使得該用戶瞭解該基準圖片在經過模糊處理之後，該基準圖片的副本的模糊程度，以增加用戶對該基準圖片的副本的記憶力的同時，讓用戶瞭解模糊處理的程度，可增加用戶對該安全問題的生成過程的理解，提高用戶使用該安全問題的意願。

當然，在本發明中，該伺服器也可不同時發送該安全問題與該是否保存該安全問題的詢問資訊，即，該伺服器可以僅發送該安全問題，並根據該終端返回的該安全問題的結果，確定是否保存該安全問題，或者該伺服器也可僅發送該是否保存該安全問題的詢問資訊，並當該終端返回

保存該安全問題的資訊時，保存該安全問題，反之亦然。

具體的，可如步驟 S10311~步驟 S10314所示，根據身份驗證結果確定是否保存安全問題：

步驟 S10311：該伺服器可以向該終端發送生成的該安全問題；

步驟 S10312：根據該終端返回的對該安全問題的答題結果，確定該終端的身份驗證結果；

步驟 S10313：當該身份驗證結果為通過時，確定保存該安全問題；

步驟 S10314：當該身份驗證結果為不通過時，刪除該安全問題。

或者，如步驟 S10321~步驟 S10324所示，根據終端返回的資訊，確定是否保存該安全問題：

步驟 S10321：向該終端發送是否保存該安全問題的詢問資訊；

步驟 S10322：當該終端返回保存該安全問題的資訊時，保存該安全問題；

步驟 S10323：當該終端返回不保存該安全問題的資訊時，刪除該安全問題。

進一步地，由於任何安全問題在長時間使用之後，隨著該安全問題使用次數的增加，該安全問題被破解的機率會越來越高，並且，若該安全問題在較長時間內沒有使用，則用戶對該安全問題的記憶也會有所下降，該安全問題的準確性下降，所以為了提高該安全問題的安全性以及

提高該安全問題的準確性，在本發明中，該伺服器還可以在生成該安全問題時，同時確定該安全問題的標識對應的有效期，並當需要使用該安全問題時，根據該安全問題的標識的有效期，判斷是否使用該安全問題，具體的，當需要使用該安全問題時，判斷該安全問題在當前時刻是否處於有效期內，若是，則該安全問題可以使用，反之亦然。

更進一步地，在現有技術中，為了提高身份驗證的準確性，通常一個帳戶標識可對應多個用於身份驗證的安全問題，而通常考慮到用戶對身份驗證過程的使用意願，現有技術不會在一次身份驗證過程中將所有的安全問題都發送至終端進行身份驗證，而可根據各安全問題的優先順序，確定一定數量的安全問題用於身份驗證。並且，可以是以當前時刻該安全問題的標識對應的優先順序越高，選擇該安全問題的標識的機率越高的方式，選擇安全問題的標識。

於是，在本發明中，當該伺服器確定該帳號對應有多個安全問題時，該伺服器還可在生成該安全問題時，設置該安全問題的標識的優先順序(即，初始設置的該安全問題的標識的優先順序)，並且該安全問題的標識初始設置的優先順序，可隨該安全問題的標識生成時間至當前時刻的時長增加而降低，直至降低到預設的基礎優先順序為止，具體過程可如圖4a或者圖4b所示。

圖4a為本發明實施例提供的安全問題的標識的優先順序隨時間變化的示意圖。其中，橫軸(即，x軸)為時間

軸，縱軸(即，y軸)表示優先順序，在y軸上越高的點對應的優先順序越高，可見當圖4中所示的安全問題的標識生成時，該安全問題的標識對應的優先順序，自x軸的初始時間點開始隨著時間的變化逐漸降低，直至基準優先順序。另外，在本發明中，對於安全問題的標識的優先順序如何隨時間降低也可以採用多種形式，如圖4b所示該安全問題的標識的優先順序不是逐漸變化的而是突變的，當然，本發明對設置的優先順序如何隨時間並不做具體限定，在實際應用過程中可根據需要進行確定。

在本發明中，由於可以採用該安全問題的標識的優先順序越高，選中該安全問題的標識的機率越高的方式，確定安全問題的標識，所以採用如圖4a-4b所示的優先順序變化的設置，可以使得該安全問題在生成之後，該安全問題被用於身份驗證的機率較高，使得該用戶可以更多的接觸到該安全問題，該以提高用戶對該安全問題的記憶力，即，優先順序數值較高的安全問題，被選為進行身份驗證的安全問題的幾率也就越高，使該用戶回答該安全問題的機率增加，並進一步的增加該用戶對該安全問題的記憶力。

另外，在本發明中，並不限定在步驟S101中該基準圖片一定是由該終端生成的，該基準圖片也可以是由該伺服器發送至該終端的。

具體的，該伺服器向該終端發送安全問題的生成指令以及若干待選圖片，以使得操作該終端的用戶選擇並確認

一張圖片作為基準圖片，則該伺服器可接收該終端根據該生成指令從該若干待選圖片中選擇並返回的圖片，作為該基準圖片。其中，該待選圖片可由工作人員進行設置，或者，是由該伺服器中該待選圖片池中確定的。當然，在本發明中，該伺服器發送的該待選圖片，可以是從該待選圖片池中確定的，也可以是該伺服器通過其他方法確定的，即，本發明不限定該若干待選圖片的確定方法或者選擇方法。

另外，在本發明步驟S102中除了上述採用通過確定該基準圖片的特徵值，以確定各混淆圖片的方法以外，該伺服器確定與該基準圖片對應的混淆圖片時，也可以採用先確定與該基準圖片對應的點陣向量，並以該點陣向量以及預設的取值策略，確定與該基準圖片對應的混淆圖片。

具體的，該伺服器可以根據該基準圖片的各像素點，對應生成一個像素矩陣，並以該像素矩陣作為點陣，確定該基準圖片對應的向量，之後，該伺服器便可根據預設的取值策略，確定混淆圖片的向量與該基準圖片的向量在該點陣中的距離範圍，並從該待選圖片池中，選擇待選圖片的向量與該基準圖片的向量的距離落入該距離範圍內的待選圖片，作為與該基準圖片對應的混淆圖片。

其中，對於像素矩陣來說，該像素矩陣中的每一個元素都可以對應該基準圖片中的一個像素點的灰階值，或者該像素矩陣中的每一個元素都可以對應該基準圖片中的多個像素點的灰階值的平均值，則通過該像素矩陣可以表示

該基準圖片的特徵。

為了方便後續操作，該伺服器還可以將像素矩陣生成為對應的向量形式，則該向量所處的向量空間維度可以是該像素矩陣的維度，也就是說在該像素矩陣對應的向量空間中，確定該基準圖片的向量。

另外，對於該預設的取值策略來說，該取值策略用於確定與該基準圖片的向量的距離既不過於接近又不過於遠離的混淆圖片的向量的距離範圍。

具體的，該取值策略可以是距離該基準圖片的向量的距離不小於預設的最小距離，且不大於預設的最大距離，則該伺服器可根據該距離範圍，在該待選圖片池中，確定在該像素矩陣對應的向量空間中，待選圖片的向量落入該距離範圍的內待選圖片，作為混淆圖片，如圖5所示。

圖5為本發明實施例提供的在向量空間中，該距離範圍、各待選圖片的向量以及該基準圖片的向量的對應關係。

可見，該向量空間由像素矩陣中的R值和B值確定，各個實心點為各待選圖片在該向量空間中的向量，空心點為該基準圖片在該向量空間中的向量，虛線所圍起的環狀區域，為該距離範圍，則落入該距離範圍內的向量所對應的待選圖片可作為與該基準圖片對應的混淆圖片。

當然，由於該基準圖片中的每個像素點都可以以紅綠藍(Red、Blue、Green，RGB)值來表示，所以該像素矩陣中的每個元素，也可以由該基準圖片中一個像素點的RGB

值的平均值、最大值或者最小值確定、由該基準圖片中一個像素點的R值確定、由該基準圖片中一個像素點的B值確定、由該基準圖片中一個像素點的G值確定。

於是，該基準圖片可以生成在多個向量空間中的多個向量，或者一個向量空間中的多個向量，例如，在RGB值對應的像素矩陣生成的向量空間中，對應一個由每個像素點的RGB值的平均值確定的向量，或者，在R值對應的像素矩陣生成的向量空間中，對應一個由每個像素點的R值確定的向量，或者，在RGB值對應的像素矩陣生成的向量空間中，對應分別由每個像素點的R值、B值以及G值確定的3個向量，等等，具體的如何生成該基準圖片的向量可以採用多種方法，本發明對此不做限定。

更進一步地，由於不同的設備生成的基準圖片的像素數量可能不一致，所以為了後續確定的混淆圖片更加準確，所以該伺服器還可以統各待選圖片以及該基準圖片的像素數量。

具體的，假設該伺服器選擇像素數量為 1600×1200 ，則當該伺服器接收該基準圖片時，可將該基準圖片的像素數量統一為 1600×1200 ，再繼續後續操作。當然，對於每個待選圖片，該伺服器可在確定該待選圖片時，便將該待選圖片的像素數量統一。當然，對於該伺服器將該基準圖片的像素數量統一為多少，本發明並不做限定，並且，該像素數量的確定可以參考對該基準圖片的圖片品質的要求而確定。

需要說明的是，本發明實施例所提供方法的各步驟的執行主體均可以是同一設備，或者，該方法也由不同設備作為執行主體。例如，步驟S101和步驟S102的執行主體可以為設備1，步驟S103的執行主體可以為設備2；又例如，步驟S101的執行主體可以為設備1，步驟S102和步驟S103的執行主體可以為設備2；等等，即，該伺服器可以是由多台設備組成的分散式伺服器。同時，本發明實施例所提供的方法的各步驟的執行主體也不限定為伺服器，也可以是終端，該終端可以是手機、個人電腦、平板電腦等設備。

基於圖1所示的安全問題的生成過程，本發明實施例還對應提供一種執行的安全問題的生成方法，如圖6所示。

圖6為本發明實施例提供的一種安全問題的生成過程，具體包括以下步驟：

S201：接收伺服器發送的安全問題的生成指令。

由於通常用戶使用終端發起或者執行業務，所以身份驗證所針對的通常也是終端上登錄的帳戶，於是在本發明實施例中，可由用戶使用的終端接收該伺服器發送的安全問題的生成指令，並根據該生成指令執行後續的操作，其中，該終端包括手機、個人電腦、平板電腦等設備。

具體的，該生成指令可包括指令碼語言(JavaScript JS)代碼，在該JS代碼中攜帶有引導資訊，該引導資訊可包括：字元、音訊以及視頻等。用於引導使用該終端的用

戶執行操作，其中，該JS代碼用於通過在該終端上運行，顯示該引導資訊，並使該終端執行後續的操作。

例如，該終端通過運行該生成指令中攜帶的JS代碼，顯示用於設置該基準圖片的設置介面，如圖6所示。

圖7為本發明實施例提供的基準圖片的設置介面示意圖，其中，可見文字說明如何設置圖片，顯示用戶繪畫結果或者拍攝結果的區域，“拍照”、“確定”和“取消”按鈕，該終端可監視用戶在該繪畫結果或者拍攝結果的區域內的手勢操作，或者用戶對各按鈕的操作。

進一步地，該引導資訊可根據實際應用情況，由工作人員設置，例如，字元資訊“請您拍攝您的錢包”、或者一段音訊資訊發出的聲音“請您拍攝您的水杯”或者一段視頻資訊播放出的畫面引導用戶繪出一張特有的圖片等等，對於該引導資訊的具體形式以及具體內容本發明不做限定。

當然，在本發明中由該終端接收該生成指令僅僅是一種實施例，在其他實施例中也可由其它設備接收該生成指令，如，區別於發送該生成指令的其他伺服器等等，為方便描述本發明後續僅以該終端為圖6所示安全問題的生成過程的執行主體進行說明。

需要說明的是，在本發明中並不限定該生成指令中一定攜帶有JS代碼，該生成指令中也可攜帶其他語言的代碼（如，C++言、C#語言等），並且該終端也可通過運行其他語言的代碼顯示該引導資訊。

S202：監測用戶的操作，並根據監測到的所述操作生成基準圖片。

在本發明實施例中，該終端可監測用戶的操作，並確定該在終端上生成的基準圖片，以便繼續執行後續步驟，使該伺服器生成該安全問題。

具體的，由於在步驟S201中，該終端通過該生成指令，可以引導使用該終端的用戶，繪畫或者拍照，所以在步驟S202中，該終端可監測該用戶的置操作，並根據監測到的該操作生成基準圖片。

該終端可監測用戶在指定區域的手勢操作，並將該手勢操作生成的圖像作為生成的該基準圖片，或者該終端可監測用戶的操作，將感測器採集的圖像作為生成的所述基準圖片。也就是說，該終端可以通過監測用戶手勢操作“畫”出的圖片，並作為該基準圖片，或者也可監測用戶的操作，將用戶操作時該終端的感測器採集的圖片作為該基準圖片，其中該感測器可以是該終端上的攝像頭，或者其他感測器，只要該感測器採集的資料可以作為一張基準圖片即可。

例如，圖7所示的介面，當該終端監測到用戶點擊“確定”按鈕的操作時，便可確定該顯示用戶繪畫結果或者拍攝結果的區域中的圖片為在該終端上生成的該基準圖片。

另外，在本發明中由於並不限制該感測器一定是圖像採集感測器，而可以是其他感測器，如，當該感測器為加

速度感測器時，該終端也可將該用戶操作時，該加速度感測採集的加速度資料進行圖像化處理後，作為該基準圖片，又或者，當該感測器為聲音感測器(如，話筒)時，該終端也可見將該用戶操作室，該聲音感測器採集的聲音音訊資料進行圖像化處理後，作為該基準圖片。

S203：向所述伺服器返回所述基準圖片，以使得所述伺服器根據所述基準圖片生成安全問題。

在本發明實施例中，該終端在確定了該基準圖片之後，便可將該基準圖片返回該伺服器，以使得該伺服器執行如圖1所示的步驟S102~S104，生成該安全問題，本發明對此不再贅述。

需要說明的是，本發明實施例所提供方法的各步驟的執行主體均可以是同一設備。

基於上述描述，本發明實施例還提供一個安全問題生成的詳細流程圖，如圖8所示。

圖8為本發明實施例提供的安全問題生成的詳細流程圖。

S301：伺服器判斷帳戶標識是否已通過身份驗證，若是執行步驟S302，若否執行步驟S318；

S302：向終端發送安全問題的生成指令；

S303：終端接收伺服器發送的安全問題的生成指令；

S304：該終端監測用戶的操作，並根據監測到的所述操作生成基準圖片；

S305：該終端向所述伺服器返回所述基準圖片；

S306：該伺服器接收該基準圖片，並判斷該基準圖片是否滿足預設條件，若是則執行步驟S307，若否則重新執行步驟S302；

S307：該伺服器將該基準圖片進行模糊處理，確定該基準圖片的副本；

S308：該伺服器確定該基準圖片對應的特徵值；

S309：該伺服器根據該特徵值，確定若干與該基準圖片對應的混淆圖片；

S310：該伺服器根據所述基準圖片的副本以及各混淆圖片，生成安全問題；

S311：該伺服器向所述終端發送生成的所述安全問題；

S312：該終端接收該安全問題，並將監測到的對該安全問題的答題結果返回至該伺服器；

S313：該伺服器根據所述終端返回的對所述安全問題的答題結果，確定所述終端的身份驗證結果；

S314：該伺服器將所述身份驗證結果以及是否保存所述安全問題的詢問資訊，發送至所述終端；

S315：該終端監測該用戶對該保存詢問資訊的選擇，並返回該伺服器；

S316：當所述終端返回保存所述安全問題的資訊時，保存所述安全問題；

S317：當所述終端返回不保存所述安全問題的資訊時，刪除所述安全問題；

S318：不生成該安全問題。

其中，需要說明的是該終端可以是手機、個人電腦等設備，該伺服器可以是單獨的一台設備，也可以是由多台設備組成的系統，並且，步驟S306中所述的判斷該基準圖片是否滿足條件的步驟，也可在後續步驟中的執行，只要在步驟S316之前執行即可，步驟S307對該基準圖片進行模糊處理的過程只要在步驟S310之前執行即可。

另外，在步驟S316或步驟S310中，當該伺服器確定生成該安全問題時，該伺服器還可保存該帳戶標識、該基準圖片、該基準圖片的副本、各混淆圖片、該安全問題的標識的對應關係，以便可以多次重複生成該安全問題。

進一步地，該步驟S308和步驟S309中，除了採用特徵值確定各混淆圖片以外，也可以採用先確定與該基準圖片對應的點陣向量，並以該點陣向量以及預設的取值策略，確定與該基準圖片對應的混淆圖片，本發明對此不再贅述。

本發明實施例還提供一種使用圖1、圖6或圖8所示方法生成的安全問題進行身份驗證的方法，如圖9所示。

圖9為本發明實施例提供的一種身份驗證方法，具體包括以下步驟：

S401：根據待驗證帳戶，確定用於生成與所述待驗證帳戶對應的安全問題的基準圖片。

在現有技術中，身份驗證的過程可以由伺服器發起，也可由終端發起，而在本發明中並不關於身份驗證如何發

起的問題，但是安全問題通常使用伺服器確定並發送至終端的，所以在本發明中，可由該伺服器確定待驗證帳戶。

其中，身份驗證通常都是針對帳戶的身份驗證，所以在本發明中，該伺服器確定的是待驗證帳戶，並且，該伺服器可根據確定的該待驗證帳戶，進一步確定用於生成安全問題的基準圖片。

具體的，該伺服器可以先確定待驗證的帳戶，之後通過已經儲存的帳戶與各基準圖片之間的對應關係，確定該待驗證帳戶對應的基準圖片，當然，若該伺服器中沒有儲存該對應關係，則說明該待驗證帳戶沒有生成對應的安全問題，或者沒有可用的安全問題，身份驗證過程結束。

S402：根據所述基準圖片以及與所述基準圖片對應的各混淆圖片，生成安全問題。

在本發明實施例中，當該伺服器確定了該待驗證帳戶對應的該基準圖片之後，便可生成該安全問題已進行後續的身份驗證過程。

具體的，該伺服器可以根據已經儲存的該基準圖片與各混淆圖片的對應關係，確定若干混淆圖片，並採用圖1所示步驟**S104**相同的方法，生成該安全問題。

另外，由於該伺服器在生成該安全問題時，保存了該安全問題的標識、該基準圖片、該基準圖片與各混淆圖片的對應關係等等資料，以便在身份驗證時可以確定該安全問題的，並且，該安全問題的標識還可以對應有有效期，撕破該伺服器在生成該安全問題之前，還可判斷當前時刻

該安全問題的標識是否處於有效期內，若是，則確定生成該安全問題，若否，則不生成該安全問題，並向該終端返回過期資訊。

進一步地，當該伺服器確定生成該安全問題時，該終端的用戶可在後續的身份驗證過程中回答該安全問題，則該用戶對該安全問題的記憶可得到一次加深，這就意味著，後續在採用該安全問題進行身份驗證時，該用戶仍然記得該安全問題的機率較高，所以在本發明中該伺服器還可延長該安全問題的標識的有效期，以延長該安全問題的使用時間。

S403：向所述待驗證帳戶所在的終端發送所述安全問題。

S404：接收所述終端返回的選擇結果，並根據所述選擇結果對所述待驗證帳戶進行身份驗證。

在本發明實施例中，該伺服器在採用圖1步驟S104所述的方法生成該安全問題後，還可將該安全問題發送至該終端，並接收所述終端返回的選擇結果，以根據該選擇結果對該待驗證帳戶進行身份驗證。

具體的，由於該安全問題的各答題選項分別對應於該基準圖片以及各混淆圖片，所以該伺服器接收的該終端返回的選擇結果也是該答題選項之一，也就是說該選擇結果不是該基準圖片就是個混淆圖片中的一張，所以該伺服器在根據該選擇結果對該待驗證帳戶進行身份驗證時，可以判斷該選擇結果與該基準圖片是否匹配，若是，則可確定

身份驗證結果為通過，若否，則可確定身份驗證結果為不通過。

當然，由於在現有技術中，為提高身份驗證的準確率，一個帳戶通常可對應多個安全問題(即，為該帳戶生成多個安全問題)，並且在進行身份驗證時，伺服器可選擇多個安全問題發送至終端，並根據該終端返回的對所有安全問題的選擇結果，進行身份驗證，所以在本發明中，該待驗證帳戶對應的安全問題也可存在多個。

另外，由於在多種情況下，都可使用身份驗證方法，驗證該待驗證帳戶是否具有繼續執行業務的許可權或者資格，所以本發明所述的身份驗證方法具體可用於登錄操作時的身份驗證、支付操作時的身份驗證、修改個人資訊時的身份驗證等等，具體何時進行身份驗證可根據實際應用時的需要確定，本發明對此並不做具體限定。

其中，對於支付操作時的身份驗證，本發明實施例中所述支付關於的技術載體，例如可以包括近場通訊(Near Field Communication，NFC)、WIFI、3G/4G/5G、POS機刷卡技術、二維碼掃碼技術、條碼掃碼技術、藍牙、紅外、短訊息(Short Message Service，SMS)、多媒體訊息(Multimedia Message Service，MMS)等，即，在執行支付操作時可以採用包括但不限於上述技術載體的支付方法，並可使用本發明所述的身份驗證方法進行身份驗證。

需要說明的是，該待驗證帳戶對應的多個安全問題中，可存在通過引導用戶預先設置安全問題的題目以及答

案，生成安全問題，或者通過採集和分析用戶的歷史行為資料，生成用於身份驗證的安全問題，或者如本發明圖1所示的方法生成的安全問題，本發明對此不做具體限定。並且，該伺服器在選擇安全問題時，可以是根據選擇的安全問題的標識，確定用於身份驗證的各安全問題。

基於上述描述，在該伺服器執行本發明步驟 S401 之前，該伺服器還可從與該待驗證帳戶對應的各安全問題的標識中，選擇基於基準圖片生成的安全問題的標識。

具體的，該伺服器可採用以下至少一種方法，選擇基於該基準圖片生成的安全問題的標識：

根據各安全問題的標識分別對應的有效期，選擇當前時刻處於有效期內的安全問題的標識，或者根據各安全問題的標識對應的冷卻期，選擇當前時刻不處於冷卻期內的安全問題的標識，或者根據各安全問題的標識對應的優先順序，選擇安全問題的標識。

其中，由於各安全問題的標識在生成時，該伺服器可為該安全問題的標識設置有效期，所以該伺服器在選擇對該待驗證帳戶進行身份驗證的安全問題時，可以選擇當前時刻處於有效期內的安全問題的標識。與已經描述過的內容同理，該伺服器在選擇當前時刻處於有效期內的安全問題的標識之後，還可延長選擇的該安全問題的標識對應的有效期，具體不在贅述。

對於安全問題的標識的冷卻期，由於同一個安全問題如果在一段時間內頻繁出現，則可能造成該安全問題的安

全性下降，所以在本發明中，該伺服器可以選擇當前時刻不在冷卻期內的安全問題的標識，並且在選擇之後，為該安全問題的標識設置對應的冷卻期，其中，該冷卻期的時長可由工作人員根據實際應用的需要設置。

同理，該伺服器可以採用優先順序越高，選擇的機率越高的方式，選擇用於身份驗證的安全問題，所以除了設置該冷卻期以外，該伺服器還可在選擇該安全問題的標識之後，降低所選擇的該安全問題的標識的優先順序，以使得該安全問題的標識在連續幾次的身份驗證的過程中，均被選擇的機率降低。

進一步地，該伺服器可針對該待驗證帳戶對應的每一個安全問題的標識，以當前時刻該安全問題的標識對應的優先順序越高，選擇該安全問題的標識的機率越高的方式，選擇安全問題的標識。其中，對各安全問題的標識初始設置的優先順序，隨各安全問題的標識生成時間至當前時刻的時長增加而降低，直至降低到預設的基礎優先順序為止。

更進一步地，當該選擇的安全問題的標識的優先順序不是基礎優先順序時，該伺服器降低該安全問題的標識的優先順序之後，還可隨時間變化逐漸恢復該優先順序，直到選擇該安全問題的標識時該安全問題的標識對應的優先順序為止，再使該安全問題的標識的優先順序隨時間變化而逐漸降低。而當該選擇的安全問題的標識的優先順序是基礎優先順序時，該伺服器降低該安全問題的標識的優先

順序之後，還可隨時間變化逐漸恢復該安全問題的標識的優先順序直到基礎優先順序為止。也就是說，該伺服器還可避免選擇安全問題的標識之後，該安全問題的標識由於優先順序一直較低而導致難以被選中的情況出現，由於該優先順序還可隨時間變化而恢復，所以當該安全問題的標識的優先順序恢復正常水準時(如，基礎優先順序時)，該伺服器選擇該安全問題的標識的機率也會恢復到正常水準。

當然，該伺服器採用上述的三種方法中的至少一種選擇的安全問題的標識可以有多個，也可以僅有一個，具體採用何種方式，本發明不做具體限定。

需要說明的是，本發明實施例所提供方法的各步驟的執行主體均可以是同一設備，或者，該方法也由不同設備作為執行主體。例如，步驟S401和步驟S402的執行主體可以為設備1，步驟S403的執行主體可以為設備2；又例如，步驟S401的執行主體可以為設備1，步驟S402和步驟S403的執行主體可以為設備2；等等，即，該伺服器可以是由多台設備組成的分散式伺服器。

基於圖9所示的身份驗證過程，本發明還提供一種安全問題的管理方法，如圖10所示。

圖10位本發明實施例提供的一種安全問題的管理方法，具體包括以下步驟：

S801：確定帳戶對應的各安全問題。

通常安全問題的管理可在伺服器中進行，所以在本發

明實施例中，可由該伺服器確定帳戶對應的各安全問題。其中，由於該伺服器可針對在該伺服器中儲存的所有帳戶進行安全問題的管理，所以在本發明中，該帳戶可以是該伺服器中儲存的任一帳戶，並且為了方便描述，後續以該帳戶對應的安全問題的管理進行說明。

具體的，假設該伺服器確定了一個需要進行安全問題管理的帳戶，則該伺服器可先確定該帳戶對應的各安全問題的標識。由於，針對任一安全問題，在該安全問題生成時，該伺服器可為該安全問題設置一個標識，以便管理和使用，並且該安全問題僅能針對某一個帳戶進行身份驗證，所以該安全問題的標識還可與帳戶存在對應關係，於是在本發明中，該伺服器可以確定該帳戶對應的各安全問題的標識。當然，本發明並不限定該伺服器僅以安全問題的標識，確定各安全問題，該伺服器也可以通過其他方式確定各安全問題，例如，該伺服器通過已儲存的各帳戶與各安全問題的對應關係，確定該帳戶對應的各安全問題等等。

S802：確定各安全問題分別對應的生成時間以及使用記錄。

在本發明中，由於各安全問題的生成時間以及使用記錄關係到各安全問題的管理，例如，一個安全問題生成後的較長時間內都沒有使用過，則用戶對該安全問題的記憶有較大機率變得不清楚，則用該安全問題進行身份驗證的準確率就無從保證，或者，一個安全問題在一天之內多次

使用，則該安全問題暴露的過於頻繁，則該安全問題的安全性有降低的可能，所以該伺服器為了管理各安全問題，需要進一步確定各安全問題分別對應的生成時間以及使用記錄。

具體的，針對每一個安全問題，由於該安全問題在生成時，生成該安全問題的伺服器還可為該安全問題生成對應的標識，即，該安全問題的標識，所以該伺服器可以根據該安全問題的標識生成時間確定該安全問題的生成時間。例如，可由該伺服器讀取該安全問題的標識對應的第一條歷史記錄，或者該安全問題的標識的生成記錄，並根據該記錄確定該安全問題的標識的生成時間，當然，該伺服器具體如何確定該安全問題的標識的生成時間本發明不做具體限定，可根據實際應用的需要而由工作人員設置。

同理，對於使用記錄可與現有技術相同，該伺服器可針對每一個安全問題，呼叫該安全問題的標識對應的使用記錄，以確定該安全問題的使用記錄。

另外，正如步驟S101中所述的，本發明並不限定採用通過安全問題的標識的生成時間和使用記錄，確定該安全問題的生成時間以及使用記錄，該伺服器也可根據該安全問題的日誌，確定該安全問題的生成時間以及使用記錄。

S803：根據各安全問題對應的生成時間以及使用記錄，確定各安全問題分別對應的有效期、優先順序以及冷卻期中的至少一種。

在本發明實施例中，針對該帳戶的每個安全問題，由

於該安全問題可對應有效期、冷卻期以及優先順序中的至少一種，並且該有效期、冷卻期以及優先順序均可通過該安全問題的生成時間以及使用記錄確定，所以該伺服器可根據步驟S802中確定的各安全問題的生成時間以及使用記錄，確定各安全問題的有效期、冷卻期以及優先順序中的至少一種。

具體的，該伺服器針對每個安全問題，根據該安全問題的生成時間至當前時刻的時長，確定當前時刻該安全問題的優先順序，其中，對該安全問題初始設置的優先順序，隨該安全問題生成時間至當前時刻的時長增加而降低，直至降低到預設的基礎優先順序為止。

針對每個安全問題，根據該安全問題對應的使用記錄，每生成一次該安全問題對應的使用記錄，該伺服器便可確定該安全問題使用了一次，則可延長一次該安全問題對應的有效期。

針對每個安全問題，根據該安全問題對應的使用記錄，每生成一次該安全問題對應的使用記錄，該伺服器便可確定該安全問題使用了一次，則可為該安全問題設置一個冷卻期。

也就是說，該伺服器可以通過該安全問題對應的使用記錄，確定該安全問題的每一次使用情況，並在該安全問題使用時，延長該安全問題對應的有效期，為該安全問題設置一個冷卻期。

另外，該伺服器除了設置冷卻期以外，如圖7所述的

身份驗證過程同理，該伺服器也可根據各安全問題的使用記錄，降低各安全問題的優先順序，如，當該選擇的安全問題的優先順序不是基礎優先順序時，該伺服器降低該安全問題的優先順序之後，該安全問題的優先順序還可隨時間變化逐漸恢復該優先順序，直到選擇該安全問題時該安全問題對應的優先順序。或者，當該選擇的安全問題的優先順序是基礎優先順序時，該伺服器降低該安全問題的優先順序之後，該安全問題的優先順序可隨時間變化逐漸恢復到基礎優先順序為止。

當然，若針對該帳戶對應的每個安全問題的標識，該安全問題的標識也對應有效期、冷卻期以及優先順序，並用以標識該安全問題的有效期、冷卻期以及優先順序，則該伺服器還可以確定該安全問題的標識的有效期、冷卻期以及優先順序中的至少一種，並以此確定該安全問題的有效期、冷卻期以及優先順序，本發明對比不做限定。

S804：當對所述帳戶進行身份驗證時，根據各安全問題分別對應的有效期、冷卻期以及優先順序中的至少一種，從所述帳戶對應的各安全問題中，選擇用於身份驗證的安全問題對所述帳戶進行身份驗證。

在本發明中，當該伺服器確定對該帳戶進行身份驗證時，該伺服器也可根據各安全問題分別對應的有效期、冷卻期以及優先順序中的至少一種，採用以下至少一種方法，從所述帳戶對應的各安全問題中，選擇用於身份驗證的安全問題：

根據各安全問題分別對應的有效期，確定當前時刻處於有效期內的安全問題，和/或根據各安全問題對應的冷卻期，確定當前時刻不處於冷卻期內的安全問題，和/或根據各安全問題對應的優先順序，以當前時刻該安全問題對應的優先順序越高，選擇該安全問題的機率越高的方式，選擇安全問題，並使用選擇的安全問題對應的安全問題對所述帳戶進行身份驗證。

具體過程可如圖8所示的身份驗證的過程，本發明對此不再贅述。

另外，在本發明實施例中，當該伺服器確定任一安全問題在當前時刻不處於有效期內時(或者，任一安全問題的標識在當前時刻不處於有效期內時)，該伺服器還可以刪除該安全問題以及該安全問題對應的安全問題，以釋放儲存空間，並且，該伺服器也可刪除該安全問題的生成時間以及使用記錄。

另外，由於在多種情況下，都可使用身份驗證方法驗證帳戶是否具有繼續執行業務的許可權或者資格，所以本發明所述的步驟S804中是對進行於支付操作的帳戶進行身份驗證性，本發明實施例中所述支付關於的技術載體，例如可以包括近場通訊(Near Field Communication，NFC)、WIFI、3G/4G/5G、POS機刷卡技術、二維碼掃碼技術、條碼掃碼技術、藍牙、紅外、短訊息(Short Message Service，SMS)、多媒體訊息(Multimedia Message Service，MMS)等。

基於圖1所示的安全問題的生成過程，本發明實施例還對應提供一種安全問題的生成裝置，如圖11所示。

圖11為本發明實施例提供的一種安全問題的生成裝置的結構示意圖，包括：

通訊模組501，向終端發送安全問題的生成指令，並接收所述終端根據所述生成指令生成並返回的基準圖片；

確定模組502，確定若干與所述基準圖片對應的混淆圖片；

生成模組503，根據所述基準圖片以及各混淆圖片，生成安全問題。

所述生成模組503，在生成所述安全問題之前，確定所述基準圖片滿足預設條件，其中，所述預設條件至少包括以下一種：

所述基準圖片的像素數量不小於預設的像素數量；所述基準圖片的儲存佔用空間不小於預設的儲存佔用空間；所述基準圖片的內容分類不屬於預設的分類。

所述確定模組502，確定所述基準圖片的特徵值，並根據所述基準圖片的特徵值，確定若干與所述基準圖片對應的混淆圖片。

所述確定模組502，根據預設的特徵提取模型，確定所述基準圖片的特徵值，其中，所述特徵提取模型包含：顏色特徵模型、圖形特徵模型、複雜度特徵模型中的至少一種，所述特徵值包含：顏色特徵值、形狀特徵值、複雜度特徵值中的至少一種。

所述確定模組 502，根據所述基準圖片的特徵值以及預設的取值策略，確定所述混淆圖片的特徵值對應的取值範圍，根據所述取值範圍，從已儲存的待選圖片池中，確定特徵值落入所述取值範圍內的待選圖片，作為與所述基準圖片對應的混淆圖片。

所述取值範圍的最大值與所述基準圖片的特徵值的差值不大於預設的最大值，所述取值範圍的最小值與所述基準圖片的特徵值的差值不小於預設的最小值，所述特徵值不在所述取值範圍內。

所述生成模組 503，從各混淆圖片中，確定指定數量的所述混淆圖片，將所述基準圖片以及確定的混淆圖片分別作為答題選項，生成安全問題。

所述生成模組 503，在生成所述安全問題之前，將所述基準圖片進行模糊處理，作為所述基準圖片的副本，向所述終端發送刪除所述基準圖片的指令，並在本地保存所述基準圖片以及所述基準圖片的副本。

所述生成模組 503，從各混淆圖片中，確定指定數量的所述混淆圖片，將所述基準圖片的副本以及確定的混淆圖片分別作為答題選項，生成與所述帳戶標識對應的安全問題。

所述裝置還包括：

測試保存模組 504，接收所述終端返回的對所述安全問題的答題結果，當所述終端返回的安全問題的答題結果與所述基準圖片匹配時，確定保存所述安全問題，當所述

終端返回的安全問題的答題結果與所述基準圖片不匹配時，確定保存所述安全問題。

所述測試保存模組504，向所述終端發送是否保存所述安全問題的詢問資訊，當所述終端返回保存所述安全問題的資訊時，保存所述安全問題，當所述終端返回不保存所述安全問題的資訊時，刪除所述安全問題。

所述通訊模組501，向所述終端發送安全問題的生成指令以及若干待選圖片，接收所述終端根據所述生成指令從所述若干待選圖片中選擇並返回的圖片，作為所述基準圖片。

具體的，上述如圖11所示的安全問題的生成裝置可以位於伺服器中，該伺服器具體可以是一台設備，也可以是由多台設備組成的系統，即，分散式伺服器。

基於圖6所示的安全問題的生成過程，本發明實施例還對應提供一種安全問題的生成裝置，如圖12所示。

圖12為本發明實施例提供的另一種安全問題的生成裝置的結構示意圖，包括：

接收模組601，接收伺服器發送的安全問題的生成指令；

監測生成模組602，監測用戶的操作，並根據監測到的所述操作生成基準圖片；

發送生成模組603，向所述伺服器返回所述基準圖片，以使得所述伺服器根據所述基準圖片生成安全問題。

所述監測生成模組603，監測用戶在指定區域的手勢

操作，並將所述手勢操作生成的圖像作為生成的所述基準圖片，或者監測用戶的操作，將感測器採集的圖像作為生成的所述基準圖片。

所述裝置還包括：

刪除模組604，所述通訊模組接收的所述伺服器發送的刪除所述基準圖片的指令，並根據所述刪除所述基準圖片的指令，將本地保存的所述基準圖片刪除。

具體的，上述如圖12所示的安全問題的生成裝置可以位於終端中，該終端可以是手機、平板電腦等設備。

基於圖9所示的身份驗證的過程，本發明實施例還對應提供一種身份驗證的裝置，如圖13所示。

圖13為本發明實施例提供的一種身份驗證的裝置的結構示意圖，包括：

確定模組701，根據待驗證帳戶，確定用於生成與所述待驗證帳戶對應的安全問題的基準圖片；

生成模組702，根據所述基準圖片以及與所述基準圖片對應的各混淆圖片，生成安全問題；

發送模組703，向所述待驗證帳戶所在的終端發送所述安全問題；

驗證模組704，接收所述終端返回的選擇結果，並根據所述選擇結果對所述待驗證帳戶進行身份驗證。

與所述待驗證帳戶對應的安全問題存在多個，所述確定模組701，在確定用於生成與所述待驗證帳戶對應的安全問題的基準圖片之前，從與所述待驗證帳戶對應的各安

全問題的標識中，選擇基於基準圖片生成的安全問題的標識。

所述確定模組701，採用以下至少一種方法，選擇基於基準圖片生成的安全問題的標識：

根據各安全問題的標識分別對應的有效期，選擇當前時刻處於有效期內的安全問題的標識；根據各安全問題的標識對應的冷卻期，選擇當前時刻不處於冷卻期內的安全問題的標識；根據各安全問題的標識對應的優先順序，選擇安全問題的標識。

所述確定模組701，在選擇當前時刻處於有效期內的安全問題的標識之後，延長選擇的所述安全問題的標識對應的有效期。

所述確定模組701，在選擇當前時刻不處於冷卻期內的安全問題的標識之後，設置選擇的所述安全問題的標識對應的冷卻期。

所述確定模組701，在選擇安全問題的標識之後，降低選擇的所述安全問題的標識對應的優先順序。

對所述安全問題的標識初始設置的優先順序，隨所述安全問題的標識生成時間至當前時刻的時長增加而降低，直至降低到預設的基礎優先順序為止。

所述確定模組701，針對每一個安全問題的標識，以當前時刻該安全問題的標識對應的優先順序越高，選擇該安全問題的標識的機率越高的方式，選擇安全問題的標識。

所述驗證模組704，接收所述終端返回的選擇結果，判斷所述選擇結果與所述基準圖片是否匹配，若是，則確定所述待驗證帳戶的身份驗證結果為通過，若否，則確定所述待驗證帳戶的身份驗證結果為不通過。

所述待驗證帳戶為執行支付操作的帳戶，所述驗證模組704，根據所述選擇結果，對所述待驗證帳戶進行身份驗證，當所述身份驗證結果通過時，執行所述支付操作，當所述身份驗證結果不通過時，拒絕所述支付操作。

具體的，上述如圖13所示的身份驗證的裝置可以位於伺服器中，該伺服器具體可以是一台設備，也可以是由多台設備組成的系統，即，分散式伺服器。

當本發明實施例提供的該身份驗證的裝置用於，對進行支付操作的帳戶身份驗證時，本發明實施例中所述支付關於的技術載體，例如可以包括近場通訊(Near Field Communication，NFC)、WIFI、3G/4G/5G、POS機刷卡技術、二維碼掃碼技術、條碼掃碼技術、藍牙、紅外、短訊息(Short Message Service，SMS)、多媒體訊息(Multimedia Message Service，MMS)等。

基於圖9所述的安全問題的管理方法，本發明實施例還對應提供一種安全問題的管理裝置，如圖13所示。

圖13為本發明實施例提供的一種安全問題的管理裝置的結構示意圖，包括：

第一確定模組901，確定帳戶對應的各安全問題；

第二確定模組902，確定各安全問題分別對應的生成

時間以及使用記錄；

第三確定模組 903，根據各安全問題對應的生成時間以及使用記錄，確定各安全問題分別對應的有效期、優先順序以及冷卻期中的至少一種；

驗證選擇模組 904，當對所述帳戶進行身份驗證時，根據各安全問題分別對應的有效期、冷卻期以及優先順序中的至少一種，從所述帳戶對應的各安全問題中，選擇用於身份驗證的安全問題對所述帳戶進行身份驗證。

所述第三確定模組 903，針對每個安全問題，根據該安全問題的生成時間至當前時刻的時長，確定當前時刻該安全問題的優先順序，其中，對該安全問題的優先順序，隨該安全問題生成時間至當前時刻的時長增加而降低，直至降低到預設的基礎優先順序為止。

所述第三確定模組 903，針對每個安全問題，根據該安全問題對應的使用記錄，每使用一次該安全問題，延長一次該安全問題對應的有效期。

所述第三確定模組 903，針對每個安全問題，根據該安全問題對應的使用記錄，每使用一次該安全問題，為該安全問題設置一個冷卻期。

驗證選擇模組 904，根據所述帳戶標識對應的各安全問題分別對應的有效期、優先順序以及冷卻期，採用以下至少一種方法，從所述帳戶對應的各安全問題中，選擇用於身份驗證的安全問題：

根據各安全問題分別對應的有效期，確定當前時刻處

於有效期內的安全問題；根據各安全問題對應的冷卻期，確定當前時刻不處於冷卻期內的安全問題；根據各安全問題對應的優先順序，以當前時刻該安全問題對應的優先順序越高，選擇該安全問題的機率越高的方式，選擇安全問題。

所述驗證選擇模組904，當確定所述安全問題不處於有效期內時，刪除所述安全問題以及所述安全問題對應的安全問題。

具體的，上述如圖13所示的身份驗證的裝置可以位於伺服器中，該伺服器具體可以是一台設備，也可以是由多台設備組成的系統，即，分散式伺服器。

另外，當本發明實施例提供的該驗證選擇模組904用於，對執行支付操作的帳戶身份驗證時，本發明實施例中所述支付關於的技術載體，例如可以包括近場通訊(Near Field Communication，NFC)、WIFI、3G/4G/5G、POS機刷卡技術、二維碼掃碼技術、條碼掃碼技術、藍牙、紅外、短訊息(Short Message Service，SMS)、多媒體訊息(Multimedia Message Service，MMS)等。

在20世紀90年代，對於一個技術的改進可以很明顯地區分是硬體上的改進(例如，對二極體、電晶體、開關等電路結構的改進)還是軟體上的改進(對於方法流程的改進)。然而，隨著技術的發展，當今的很多方法流程的改進已經可以視為硬體電路結構的直接改進。設計人員幾乎都通過將改進的方法流程程式設計到硬體電路中來得到相

應的硬體電路結構。因此，不能說一個方法流程的改進就不能用硬體實體模組來實現。例如，可程式設計邏輯裝置(Programmable Logic Device, PLD)(例如現場可程式設計閘陣列(Field Programmable Gate Array, FPGA))就是這樣一種積體電路，其邏輯功能由用戶對裝置程式設計來確定。由設計人員自行程式設計來把一個數位系統“整合”在一片PLD上，而不需要請晶片製造廠商來設計和製作專用的積體電路晶片。而且，如今，取代手工地製作積體電路晶片，這種程式設計也多半改用“邏輯編譯器(logic compiler)”軟體來實現，它與程式開發撰寫時所用的軟體編譯器相類似，而要編譯之前的原始代碼也得用特定的程式設計語言來撰寫，此稱之為硬體描述語言(Hardware Description Language, HDL)，而HDL也並非僅有一種，而是有許多種，如ABEL(Advanced Boolean Expression Language)、AHDL(Altera Hardware Description Language)、Confluence、CUPL(Cornell University Programming Language)、HDCal、JHDL(Java Hardware Description Language)、Lava、Lola、MyHDL、PALASM、RHDL(Ruby Hardware Description Language)等，目前最普遍使用的是VHDL(Very-High-Speed Integrated Circuit Hardware Description Language)與Verilog。本領域技術人員也應該清楚，只需要將方法流程用上述幾種硬體描述語言稍作邏輯程式設計並程式設計到積體電路中，就可以很容易得到實現該邏輯方法流程的硬

體電路。

控制器可以按任何適當的方式實現，例如，控制器可以採取例如微處理器或處理器以及儲存可由該(微)處理器執行的電腦可讀程式碼(例如軟體或韌體)的電腦可讀媒體、邏輯閘、開關、專用積體電路(Application Specific Integrated Circuit, ASIC)、可程式設計邏輯控制器和嵌入微控制器的形式，控制器的例子包括但不限於以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及Silicone Labs C8051F320，記憶體控制器還可以被實現為記憶體的Control Logic的一部分。本領域技術人員也知道，除了以純電腦可讀程式碼方式實現控制器以外，完全可以通過將方法步驟進行邏輯程式設計來使得控制器以邏輯閘、開關、專用積體電路、可程式設計邏輯控制器和嵌入微控制器等的形式來實現相同功能。因此這種控制器可以被認為是一種硬體部件，而對其內包括的用於實現各種功能的裝置也可以視為硬體部件內的結構。或者甚至，可以將用於實現各種功能的裝置視為既可以是實現方法的軟體模組又可以是硬體部件內的結構。

上述實施例闡明的系統、裝置、模組或單元，具體可以由電腦晶片或實體實現，或者由具有某種功能的產品來實現。一種典型的實現設備為電腦。具體的，電腦例如可以為個人電腦、膝上型電腦、蜂巢式電話、相機電話、智慧型電話、個人數位助理、媒體播放機、導航設備、電子郵件設備、遊戲控制台、平板電腦、可穿戴設備或者這些

設備中的任何設備的組合。

為了描述的方便，描述以上裝置時以功能分為各種單元分別描述。當然，在實施本發明時可以把各單元的功能在同一個或多個軟體和/或硬體中實現。

本領域內的技術人員應明白，本發明的實施例可提供為方法、系統、或電腦程式產品。因此，本發明可採用完全硬體實施例、完全軟體實施例、或結合軟體和硬體態樣的實施例的形式。而且，本發明可採用在一個或多個其中包含有電腦可用程式碼的電腦可用儲存媒體(包括但不限於磁碟記憶體、CD-ROM、光學記憶體等)上實施的電腦程式產品形式。

本發明是參照根據本發明實施例的方法、設備(系統)、和電腦程式產品的流程圖和/或方塊圖來描述的。應理解可由電腦程式指令實現流程圖和/或方塊圖中的每一流程和/或方塊、以及流程圖和/或方塊圖中的流程和/或方塊的結合。可提供這些電腦程式指令到通用電腦、專用電腦、嵌入式處理機或其他可程式設計資料處理設備的處理器以產生一個機器，使得通過電腦或其他可程式設計資料處理設備的處理器執行的指令產生用於實現在流程圖一個流程或多個流程和/或方塊圖一個方塊或多個方塊中指定的功能的裝置。

這些電腦程式指令也可儲存在能引導電腦或其他可程式設計資料處理設備以特定方式工作的電腦可讀記憶體中，使得儲存在該電腦可讀記憶體中的指令產生包括指令

裝置的製造品，該指令裝置實現在流程圖一個流程或多個流程和/或方塊圖一個方塊或多個方塊中指定的功能。

這些電腦程式指令也可裝載到電腦或其他可程式設計資料處理設備上，使得在電腦或其他可程式設計設備上執行一系列操作步驟以產生電腦實現的處理，從而在電腦或其他可程式設計設備上執行的指令提供用於實現在流程圖一個流程或多個流程和/或方塊圖一個方塊或多個方塊中指定的功能的步驟。

在一個典型的配置中，計算設備包括一個或多個處理器(CPU)、輸入/輸出介面、網路介面和記憶體。

記憶體可能包括電腦可讀媒體中的非永久性記憶體，隨機存取記憶體(RAM)和/或非揮發性記憶體等形式，如唯讀記憶體(ROM)或快閃記憶體(flash RAM)。記憶體是電腦可讀媒體的實例。

電腦可讀媒體包括永久性和非永久性、可移動和非可移動媒體可以由任何方法或技術來實現資訊儲存。資訊可以是電腦可讀指令、資料結構、程式的模組或其他資料。電腦的儲存媒體的例子包括，但不限於相變記憶體(PRAM)、靜態隨機存取記憶體(SRAM)、動態隨機存取記憶體(DRAM)、其他類型的隨機存取記憶體(RAM)、唯讀記憶體(ROM)、電可抹除可程式設計唯讀記憶體(EEPROM)、快閃記憶體或其他記憶體技術、唯讀光碟唯讀記憶體(CD-ROM)、數位多功能光碟(DVD)或其他光學儲存、磁盒式磁帶，磁帶磁磁片儲存或其他磁性存放裝置

或任何其他非傳輸媒體，可用於儲存可以被計算設備存取的資訊。按照本文中的界定，電腦可讀媒體不包括暫存電腦可讀媒體 (transitory media)，如調變的資料訊號和載波。

還需要說明的是，用語“包括”、“包含”或者任何其他變體意在涵蓋非排他性的包含，從而使得包括一系列要素的過程、方法、商品或者設備不僅包括那些要素，而且還包括沒有明確列出的其他要素，或者是還包括為這種過程、方法、商品或者設備所固有的要素。在沒有更多限制的情況下，由語句“包括一個……”限定的要素，並不排除在包括所述要素的過程、方法、商品或者設備中還存在另外的相同要素。

本領域技術人員應明白，本發明的實施例可提供為方法、系統或電腦程式產品。因此，本發明可採用完全硬體實施例、完全軟體實施例或結合軟體和硬體態樣的實施例的形式。而且，本發明可採用在一個或多個其中包含有電腦可用程式碼的電腦可用儲存媒體(包括但不限於磁碟記憶體、CD-ROM、光學記憶體等)上實施的電腦程式產品的形式。

本發明可以在由電腦執行的電腦可執行指令的一般上下文中描述，例如程式模組。一般地，程式模組包括執行特定任務或實現特定抽象資料類型的常式、程式、物件、元件、資料結構等等。也可以在分散式運算環境中實踐本發明，在這些分散式運算環境中，由通過通訊網路而被連

接的遠端處理設備來執行任務。在分散式運算環境中，程式模組可以位於包括存放裝置在內的本地和遠端電腦儲存媒體中。

本說明書中的各個實施例均採用遞進的方式描述，各個實施例之間相同相似的部分互相參見即可，每個實施例重點說明的都是與其他實施例的不同之處。尤其，對於系統實施例而言，由於其基本相似於方法實施例，所以描述的比較簡單，相關之處參見方法實施例的部分說明即可。

以上所述僅為本發明的實施例而已，並不用於限制本發明。對於本領域技術人員來說，本發明可以有各種更改和變化。凡在本發明的精神和原理之內所作的任何修改、等同替換、改進等，均應包含在本發明的申請專利範圍的範圍之內。

【符號說明】

S101～S103：步驟

S1031～S1035：步驟

S201～S203：步驟

S301～S318：步驟

S401～S404：步驟

S801～S804：步驟

501：通訊模組

502：確定模組

503：生成模組

504：測試保存模組

601：接收模組

602：監測生成模組

603：發送生成模組

604：刪除模組

701：確定模組

702：生成模組

703：發送模組

704：驗證模組

901：第一確定模組

902：第二確定模組

903：第三確定模組

904：驗證選擇模組



I684886

【發明摘要】

【中文發明名稱】

安全問題的生成以及身份驗證的方法及裝置

【中文】

本發明揭露了一種安全問題的生成以及身份驗證的方法及裝置，在生成安全問題時，首先，向終端發送安全問題的生成指令，以使得該終端返回在用戶操作下生成的基準圖片，其次，根據該基準圖片，確定若干與該基準圖片對應的混淆圖片，最後，根據該基準圖片以及各混淆圖片，生成安全問題，並當需要時使用該安全問題進行身份驗證。可見，由於該安全問題是基於該基準圖片生成的，而該基準圖片是在用戶的操作下生成的，所以提高了用戶在生成安全問題時的參與度，提高了用戶對該安全問題的記憶效果，提高了該安全問題的易用性，且無需採集分析用戶的行為資料，降低了生成成本，提高了身份驗證的效率。

【指定代表圖】第(1)圖。

【代表圖之符號簡單說明】無

【特徵化學式】無

【發明圖式】

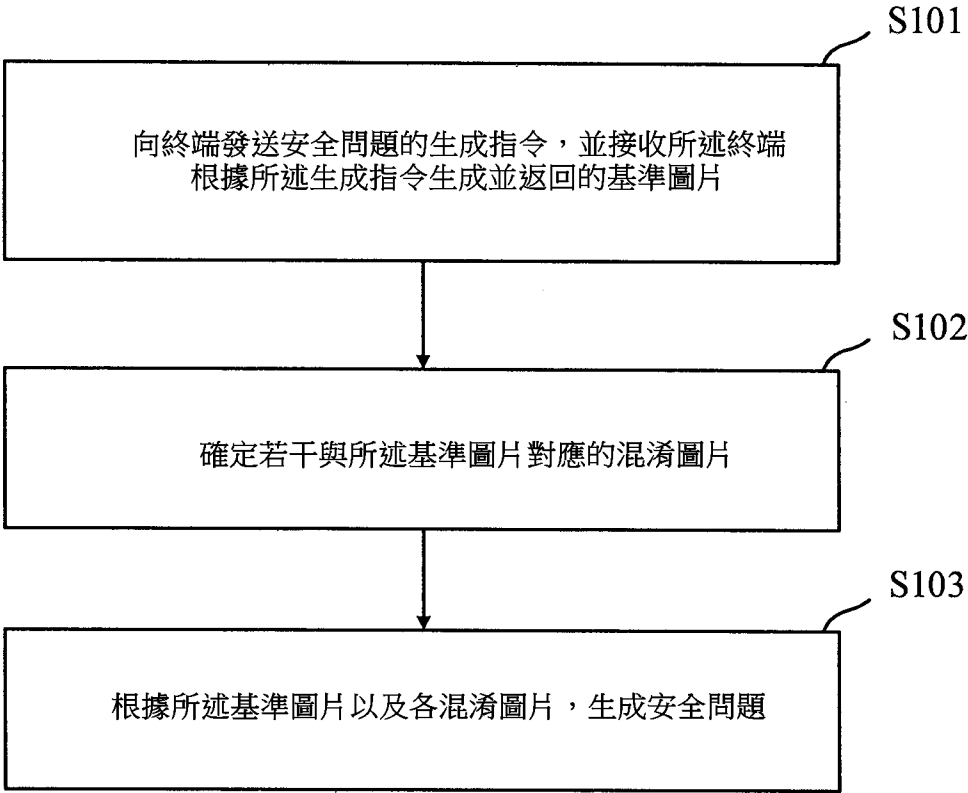


圖 1

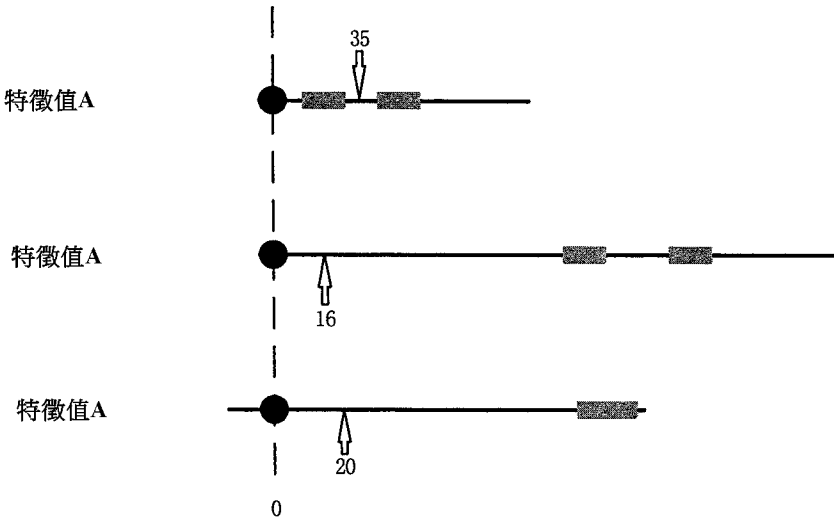


圖 2

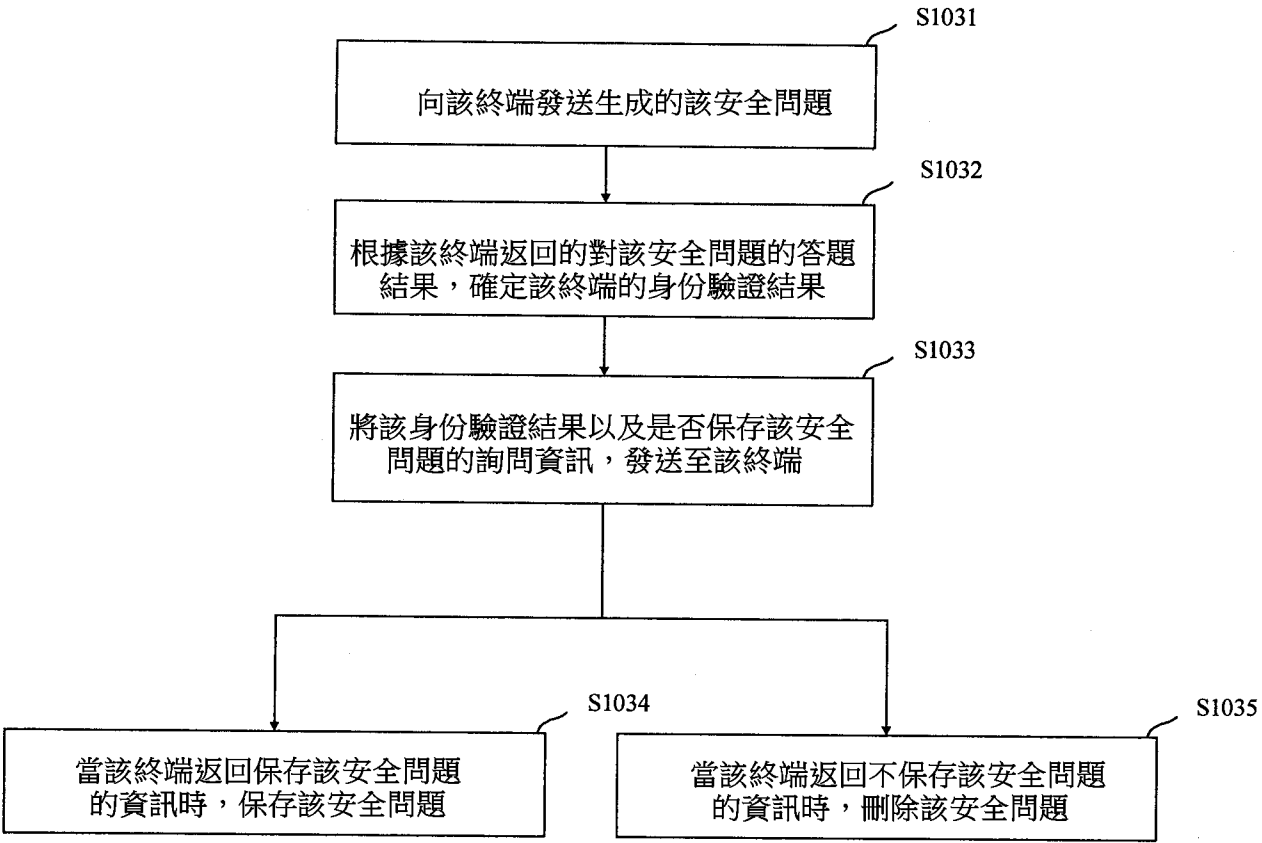


圖 3

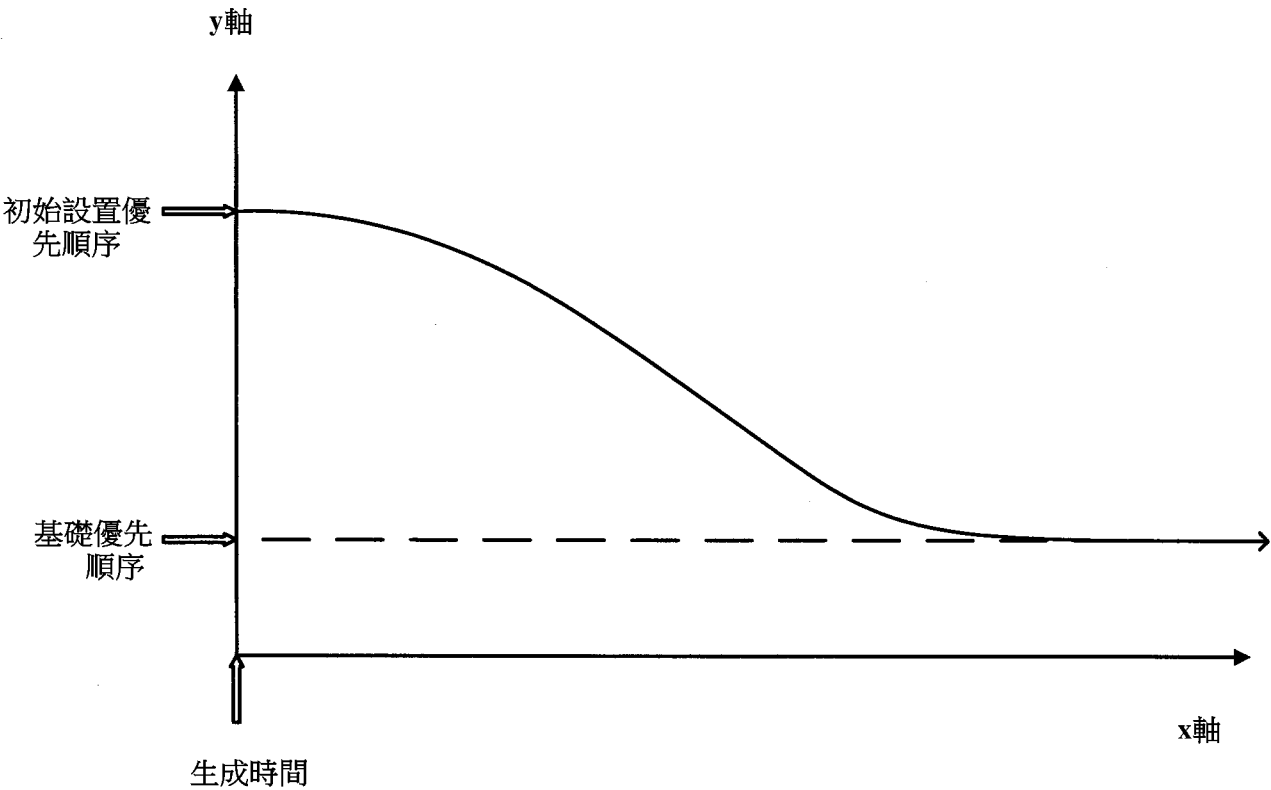


圖 4a

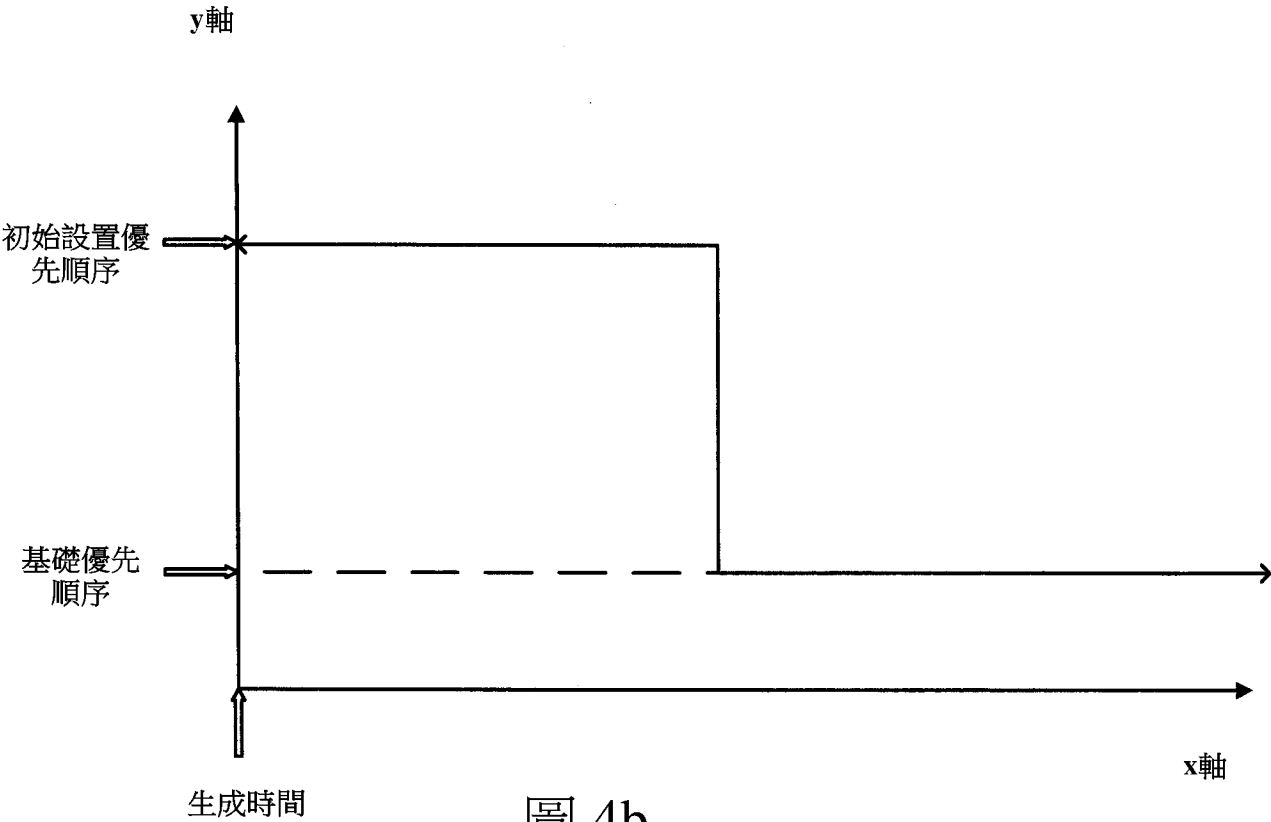


圖 4b

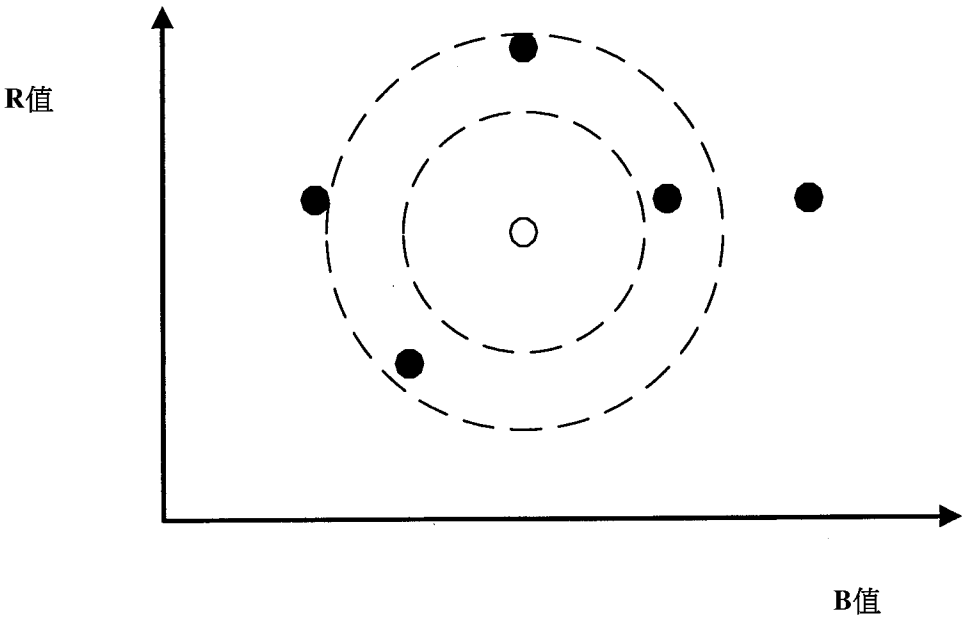


圖 5

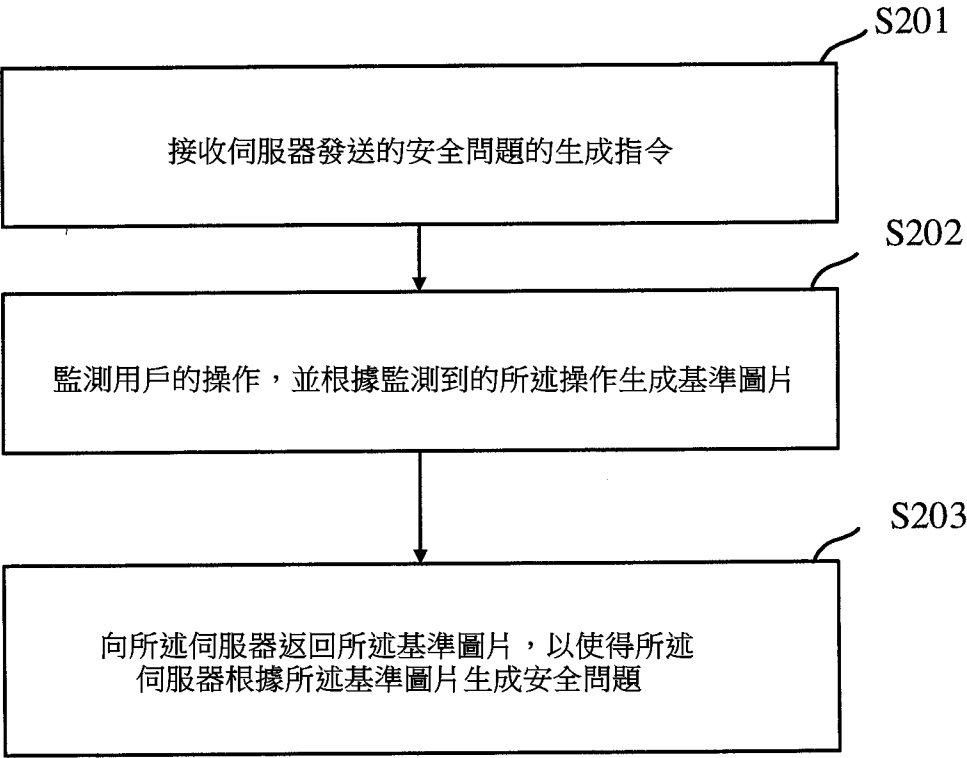


圖 6

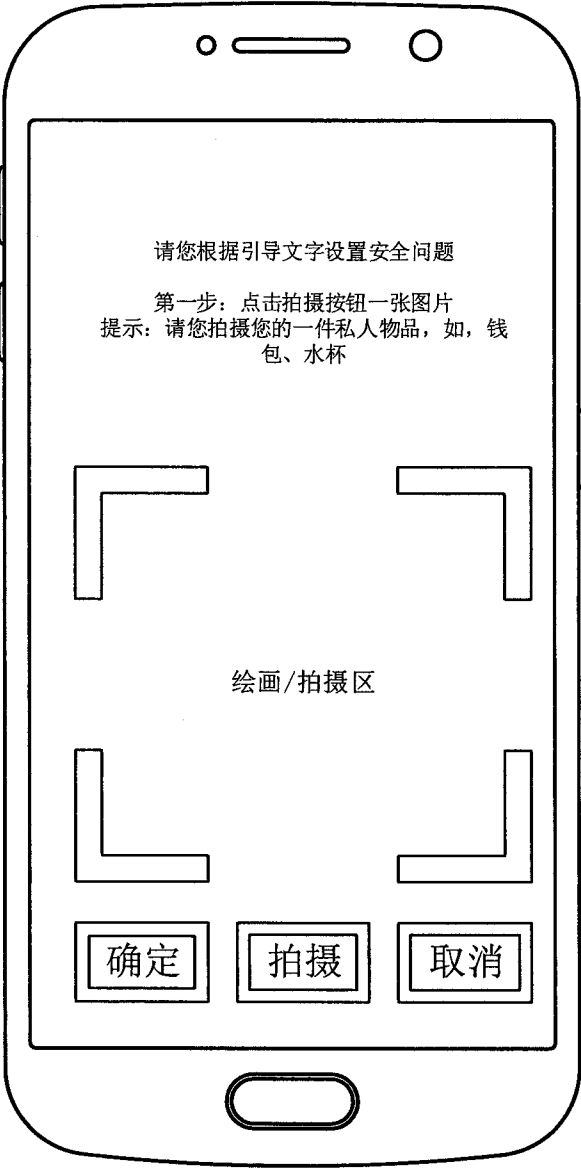


圖 7

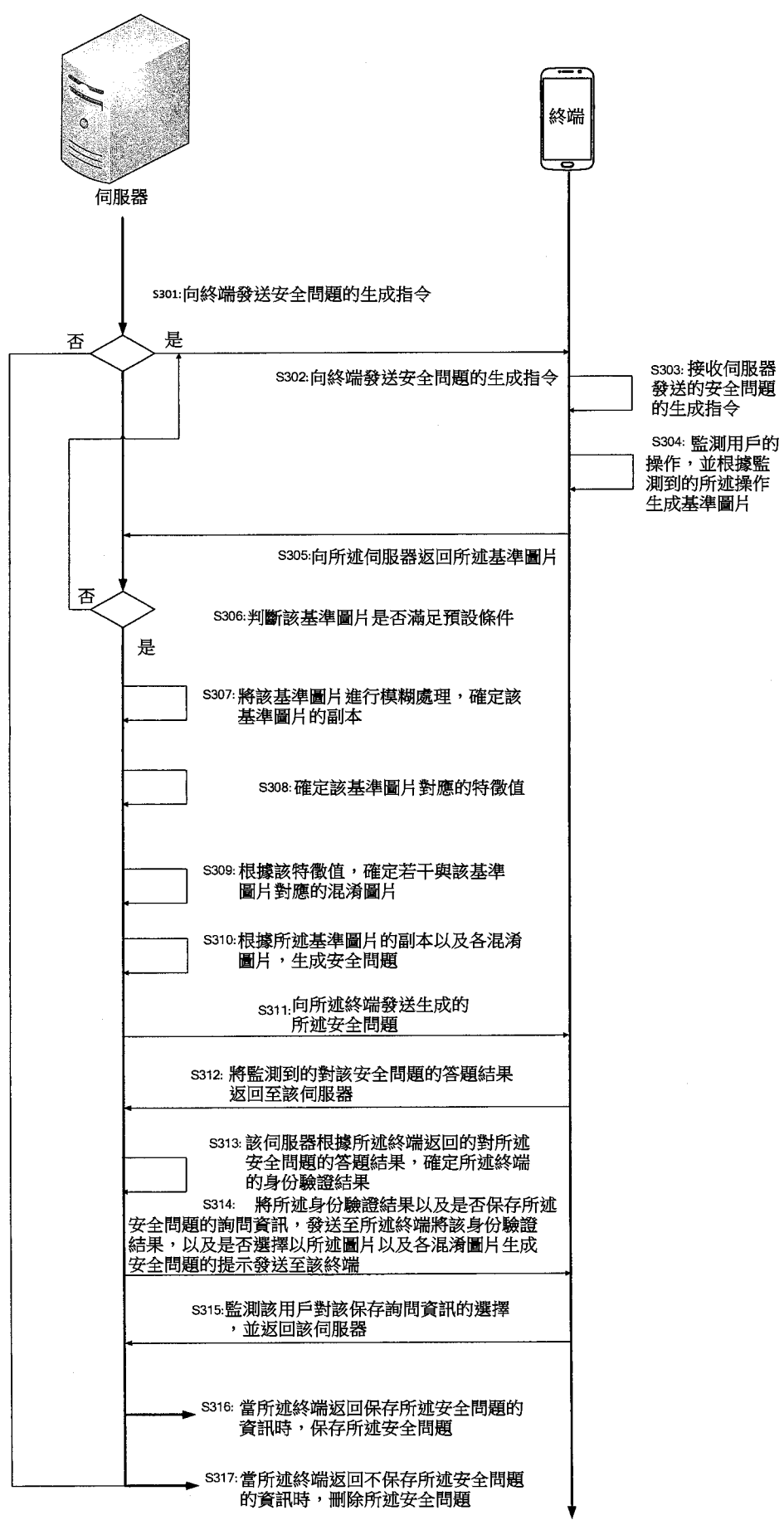


圖 8

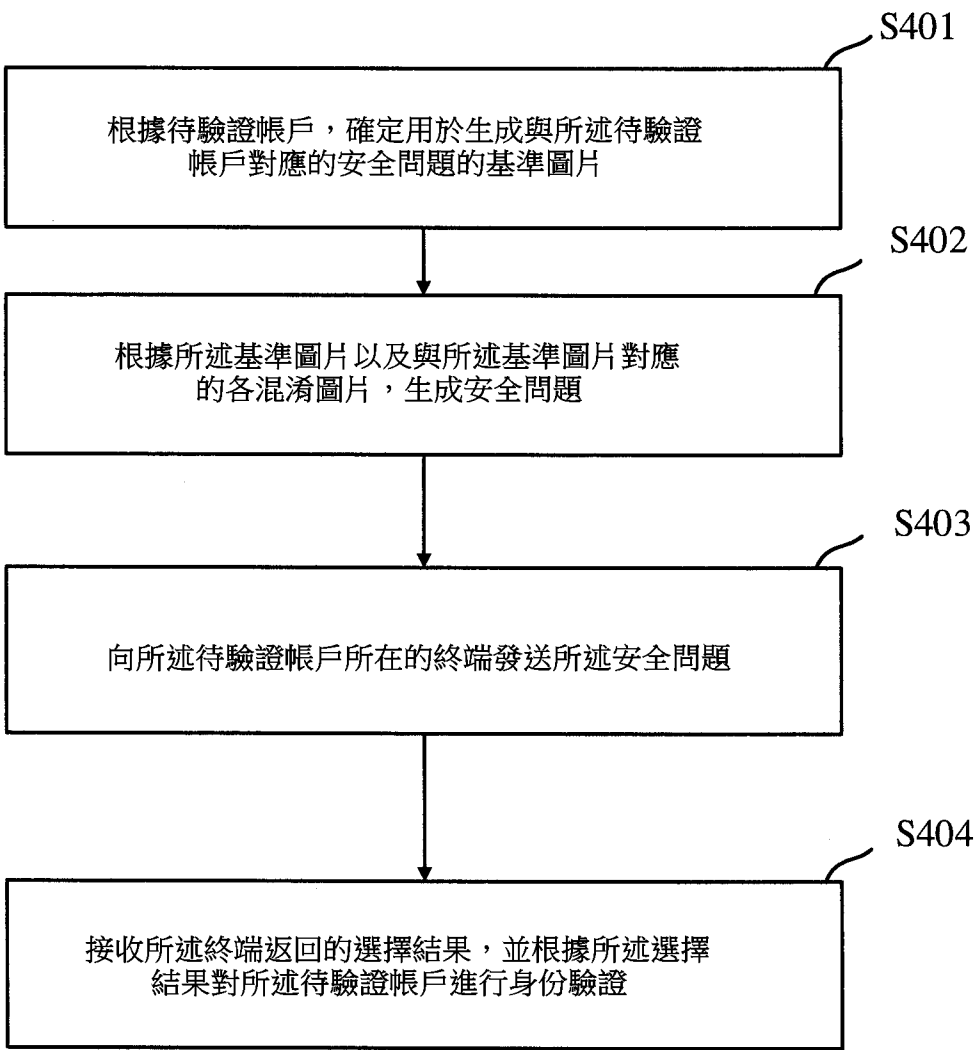


圖 9

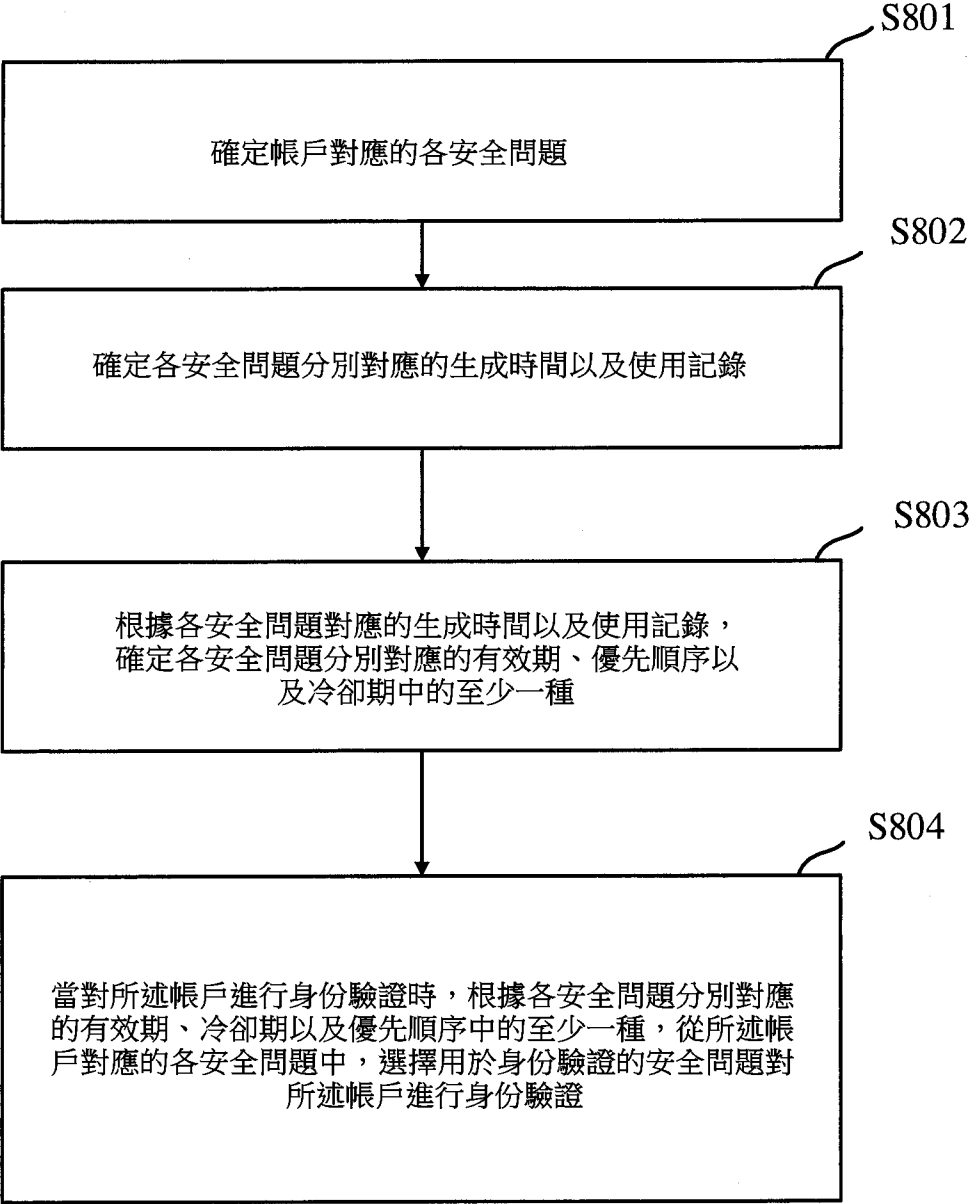


圖 10

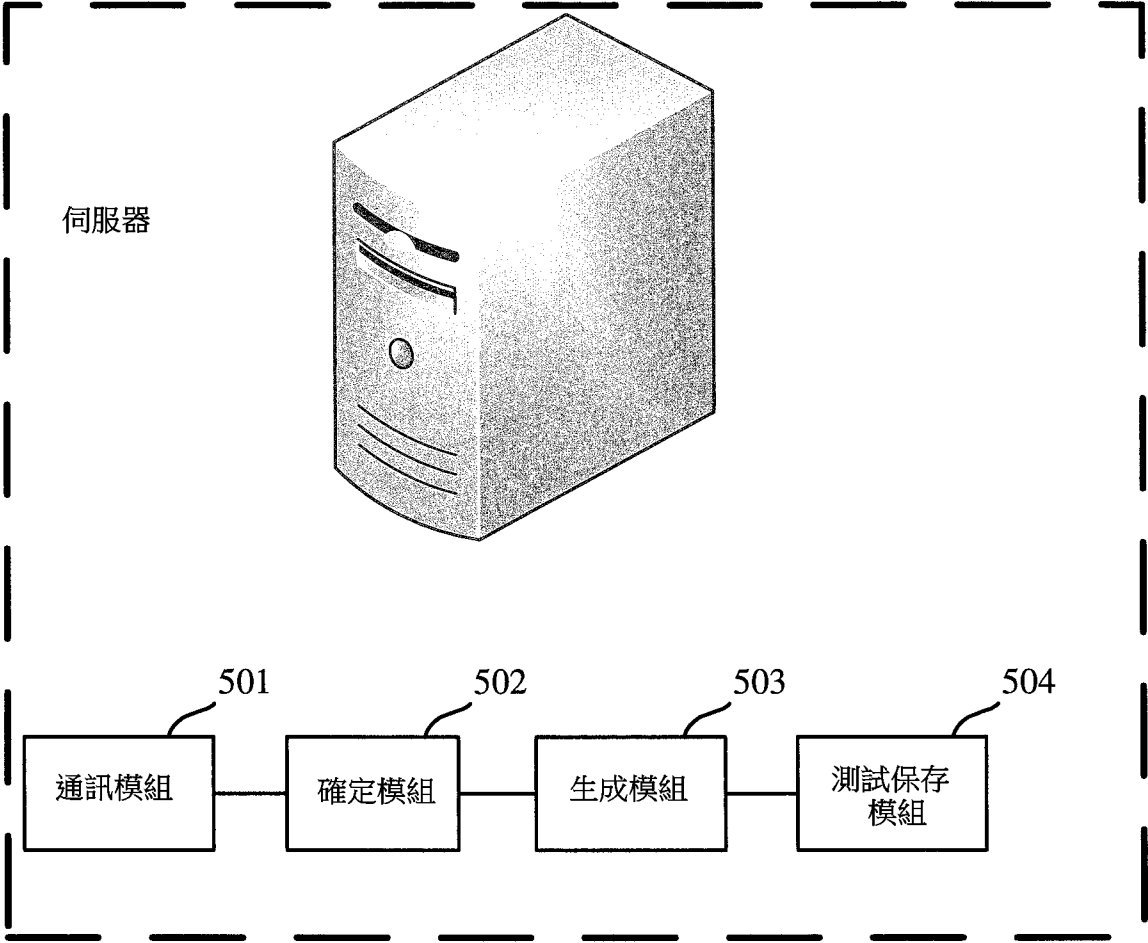


圖 11

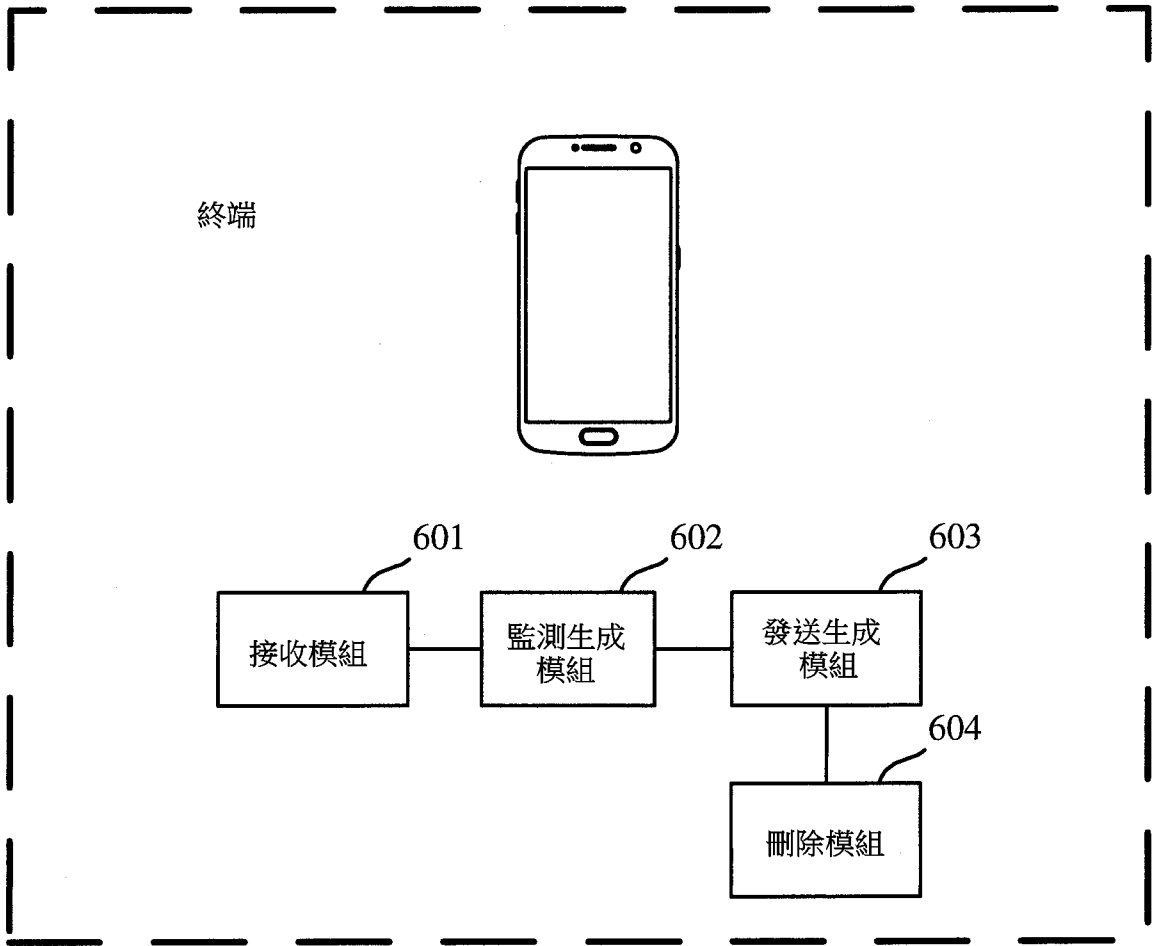


圖 12

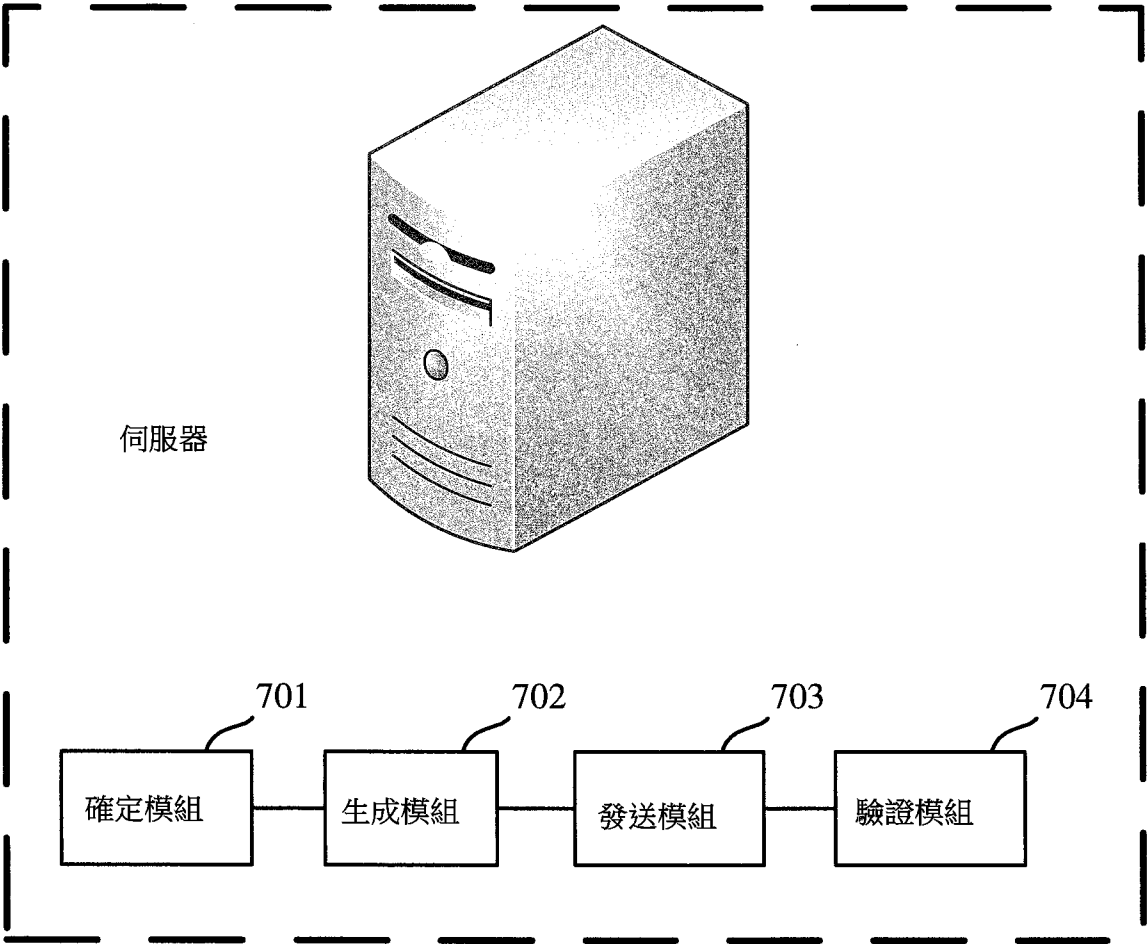


圖 13

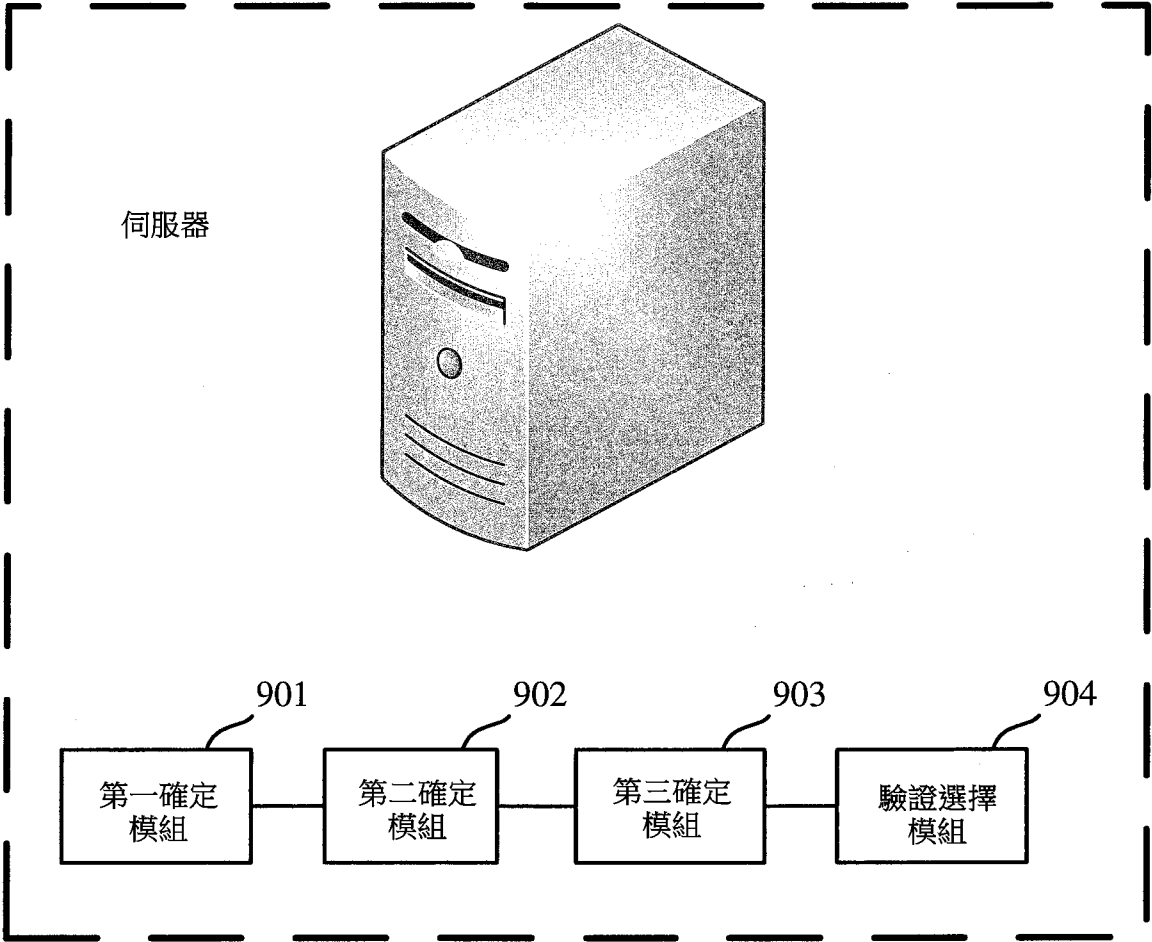


圖 14

【發明申請專利範圍】

【第1項】

一種安全問題的生成方法，應用在伺服器，所述方法包括：

向終端發送安全問題的生成指令，並接收所述終端根據所述生成指令生成並返回的基準圖片；

確定若干與所述基準圖片對應的混淆圖片；

根據所述基準圖片以及各混淆圖片，生成安全問題；

向所述終端發送生成的所述安全問題；

接收所述終端返回的對所述安全問題的答題結果；

確定所述答題結果與所述基準圖片是否匹配。

【第2項】

如申請專利範圍第1項所述的方法，其中，生成安全問題之前，所述方法還包括：

確定所述基準圖片滿足預設條件；

其中，所述預設條件至少包括以下一種：

所述基準圖片的像素數量不小於預設的像素數量；

所述基準圖片的儲存佔用空間不小於預設的儲存佔用空間；

所述基準圖片的內容分類不屬於預設的分類。

【第3項】

如申請專利範圍第1項所述的方法，其中，確定若干與所述基準圖片對應的混淆圖片，具體包括：

確定所述基準圖片的特徵值；

根據所述基準圖片的特徵值，確定若干與所述基準圖片對應的混淆圖片。

【第4項】

如申請專利範圍第3項所述的方法，其中，確定所述基準圖片的特徵值，具體包括：

根據預設的特徵提取模型，確定所述基準圖片的特徵值；

其中，所述特徵提取模型包含：顏色特徵模型、圖形特徵模型、複雜度特徵模型中的至少一種，所述特徵值包含：顏色特徵值、形狀特徵值、複雜度特徵值中的至少一種。

【第5項】

如申請專利範圍第3項所述的方法，其中，確定若干與所述基準圖片對應的混淆圖片，具體包括：

根據所述基準圖片的特徵值以及預設的取值策略，確定所述混淆圖片的特徵值對應的取值範圍；

根據所述取值範圍，從已儲存的待選圖片池中，確定特徵值落入所述取值範圍內的待選圖片，作為與所述基準圖片對應的混淆圖片。

【第6項】

如申請專利範圍第5項所述的方法，其中，所述取值範圍的最大值與所述基準圖片的特徵值的差值不大於預設的最大值，所述取值範圍的最小值與所述基準圖片的特徵值的差值不小於預設的最小值，所述特徵值不在所述取值

範圍內。

【第7項】

如申請專利範圍第1項所述的方法，其中，生成安全問題之前，所述方法還包括：

將所述基準圖片進行模糊處理，作為所述基準圖片的副本；

向所述終端發送刪除所述基準圖片的指令，並在本地保存所述基準圖片以及所述基準圖片的副本。

【第8項】

如申請專利範圍第1項所述的方法，其中，所述方法還包括：

當所述終端返回的安全問題的答題結果與所述基準圖片匹配時，確定保存所述安全問題；

當所述終端返回的安全問題的答題結果與所述基準圖片不匹配時，刪除所述安全問題。

【第9項】

如申請專利範圍第1項所述的方法，其中，所述方法還包括：

向所述終端發送是否保存所述安全問題的詢問資訊；

當所述終端返回保存所述安全問題的資訊時，保存所述安全問題；當所述終端返回不保存所述安全問題的資訊時，刪除所述安全問題。

【第10項】

如申請專利範圍第1項所述的方法，其中，向終端發

送安全問題的生成指令，並接收所述終端根據所述生成指令生成並返回的基準圖片，具體包括：

向所述終端發送安全問題的生成指令以及若干待選圖片，接收所述終端根據所述生成指令從所述若干待選圖片中選擇並返回的圖片，作為所述基準圖片。

【第11項】

一種安全問題的生成方法，應用在終端，所述方法包括：

接收伺服器發送的安全問題的生成指令；

監測用戶的操作，並根據監測到的所述操作生成基準圖片；

向所述伺服器返回所述基準圖片，以使得所述伺服器根據所述基準圖片生成安全問題；

接收所述伺服器生成的所述安全問題；

向所述伺服器返回對所述安全問題的答題結果，以使得所述伺服器確定所述答題結果與所述基準圖片是否匹配。

【第12項】

如申請專利範圍第11項所述的方法，其中，監測用戶的操作，並根據監測到的所述操作生成基準圖片，具體包括：

監測用戶在指定區域的手勢操作，並將所述手勢操作生成的圖像作為生成的所述基準圖片；或者

監測用戶的操作，將感測器採集的圖像作為生成的所

述基準圖片。

【第 13 項】

如申請專利範圍第 11 項所述的方法，其中，所述方法還包括：

接收所述伺服器發送的刪除所述基準圖片的指令；

根據所述刪除所述基準圖片的指令，將本地保存的所述基準圖片刪除。

【第 14 項】

一種身份驗證的方法，應用在伺服器，所述方法包括：

根據待驗證帳戶，確定用於生成與所述待驗證帳戶對應的安全問題的基準圖片；

根據所述基準圖片以及與所述基準圖片對應的各混淆圖片，生成安全問題；

向所述待驗證帳戶所在的終端發送所述安全問題；

接收所述終端返回的選擇結果，並根據所述選擇結果對所述待驗證帳戶進行身份驗證；

接收所述終端返回的選擇結果；

判斷所述選擇結果與所述基準圖片是否匹配。

【第 15 項】

如申請專利範圍第 14 項所述的方法，其中，與所述待驗證帳戶對應的安全問題存在多個；

在確定用於生成與所述待驗證帳戶對應的安全問題的基準圖片之前，所述方法還包括：

從與所述待驗證帳戶對應的各安全問題的標識中，選擇基於基準圖片生成的安全問題的標識。

【第16項】

如申請專利範圍第15項所述的方法，其中，從與所述待驗證帳戶對應的各安全問題的標識中，選擇基於基準圖片生成的安全問題的標識，具體包括：

採用以下至少一種方法，選擇基於基準圖片生成的安全問題的標識：

根據各安全問題的標識分別對應的有效期，選擇當前時刻處於有效期內的安全問題的標識；

根據各安全問題的標識對應的冷卻期，選擇當前時刻不處於冷卻期內的安全問題的標識；

根據各安全問題的標識對應的優先順序，選擇安全問題的標識。

【第17項】

如申請專利範圍第16項所述的方法，其中，在選擇當前時刻處於有效期內的安全問題的標識之後，所述方法還包括：

延長選擇的所述安全問題的標識對應的有效期。

【第18項】

如申請專利範圍第16項所述的方法，其中，在選擇當前時刻不處於冷卻期內的安全問題的標識之後，所述方法還包括：

設置選擇的所述安全問題的標識對應的冷卻期。

【第19項】

如申請專利範圍第16項所述的方法，其中，在選擇安全問題的標識之後，所述方法還包括：

降低選擇的所述安全問題的標識對應的優先順序。

【第20項】

如申請專利範圍第16項所述的方法，其中，對所述安全問題的標識初始設置的優先順序，隨所述安全問題的標識生成時間至當前時刻的時長增加而降低，直至降低到預設的基礎優先順序為止。

【第21項】

如申請專利範圍第16項所述的方法，其中，根據各安全問題的標識對應的優先順序，選擇安全問題的標識，具體包括：

針對每一個安全問題的標識，以當前時刻該安全問題的標識對應的優先順序越高，選擇該安全問題的標識的機率越高的方式，選擇安全問題的標識。

【第22項】

如申請專利範圍第14項所述的方法，其中，根據所述選擇結果對所述待驗證帳戶進行身份驗證，具體包括：

當所述選擇結果與所述基準圖片匹配時，則確定所述待驗證帳戶的身份驗證結果為通過；

當所述選擇結果與所述基準圖片不匹配時，則確定所述待驗證帳戶的身份驗證結果為不通過。

【第23項】

如申請專利範圍第14項所述的方法，其中，所述待驗證帳戶為執行支付操作的帳戶；

根據所述選擇結果對所述待驗證帳戶進行身份驗證，具體包括：

根據所述選擇結果，對所述待驗證帳戶進行身份驗證；

當所述身份驗證結果通過時，執行所述支付操作；

當所述身份驗證結果不通過時，拒絕所述支付操作。

【第24項】

一種安全問題的管理方法，應用在伺服器，所述方法包括：

確定帳戶對應的各安全問題；

確定各安全問題分別對應的生成時間以及使用記錄；

根據各安全問題對應的生成時間以及使用記錄，確定各安全問題分別對應的有效期、優先順序以及冷卻期中的至少一種；

當對所述帳戶進行身份驗證時，根據各安全問題分別對應的有效期、冷卻期以及優先順序中的至少一種，從所述帳戶對應的各安全問題中，選擇用於身份驗證的安全問題對所述帳戶進行身份驗證。

【第25項】

如申請專利範圍第24項所述的方法，其中，確定各安全問題分別對應的優先順序，具體包括：

針對每個安全問題，根據該安全問題的生成時間至當

前時刻的時長，確定當前時刻該安全問題的優先順序；

其中，對該安全問題的優先順序，隨該安全問題生成時間至當前時刻的時長增加而降低，直至降低到預設的基礎優先順序為止。

【第26項】

如申請專利範圍第24項所述的方法，其中，確定各安全問題分別對應的有效期，具體包括：

針對每個安全問題，根據該安全問題對應的使用記錄，每使用一次該安全問題，延長一次該安全問題對應的有效期。

【第27項】

如申請專利範圍第24項所述的方法，其中，確定各安全問題分別對應的冷卻期，具體包括：

針對每個安全問題，根據該安全問題對應的使用記錄，每使用一次該安全問題，為該安全問題設置一個冷卻期。

【第28項】

如申請專利範圍第24項所述的方法，其中，根據各安全問題分別對應的有效期、冷卻期以及優先順序中的至少一種，從所述帳戶對應的各安全問題中，選擇用於身份驗證的安全問題，具體包括：

根據所述帳戶對應的各安全問題分別對應的有效期、優先順序以及冷卻期，採用以下至少一種方法，從所述帳戶對應的各安全問題中，選擇用於身份驗證的安全問題：

根據各安全問題分別對應的有效期，確定當前時刻處於有效期內的安全問題；

根據各安全問題對應的冷卻期，確定當前時刻不處於冷卻期內的安全問題；

根據各安全問題對應的優先順序，以當前時刻該安全問題對應的優先順序越高，選擇該安全問題的機率越高的方式，選擇安全問題。

【第29項】

如申請專利範圍第28項所述的方法，其中，當確定所述安全問題不處於有效期內時，所述方法還包括：

刪除所述安全問題。

【第30項】

一種安全問題的生成裝置，包括：

通訊模組，向終端發送安全問題的生成指令，並接收所述終端根據所述生成指令生成並返回的基準圖片；

確定模組，確定若干與所述基準圖片對應的混淆圖片；

生成模組，根據所述基準圖片以及各混淆圖片，生成安全問題；

測試保存模組，向所述終端發送生成的所述安全問題，接收所述終端返回的對所述安全問題的答題結果，確定所述答題結果與所述基準圖片是否匹配。

【第31項】

如申請專利範圍第30項所述的裝置，其中，所述生成

模組，在生成所述安全問題之前，確定所述基準圖片滿足預設條件，其中，所述預設條件至少包括以下一種：

所述基準圖片的像素數量不小於預設的像素數量；所述基準圖片的儲存佔用空間不小於預設的儲存佔用空間；所述基準圖片的內容分類不屬於預設的分類。

【第32項】

如申請專利範圍第30項所述的裝置，其中，所述確定模組，確定所述基準圖片的特徵值，並根據所述基準圖片的特徵值，確定若干與所述基準圖片對應的混淆圖片。

【第33項】

如申請專利範圍第32項所述的裝置，其中，所述特徵值確定模組，根據預設的特徵提取模型，確定所述基準圖片的特徵值，其中，所述特徵提取模型包含：顏色特徵模型、圖形特徵模型、複雜度特徵模型中的至少一種，所述特徵值包含：顏色特徵值、形狀特徵值、複雜度特徵值中的至少一種。

【第34項】

如申請專利範圍第32項所述的裝置，其中，所述混淆圖片確定模組，根據所述基準圖片的特徵值以及預設的取值策略，確定所述混淆圖片的特徵值對應的取值範圍，根據所述取值範圍，從已儲存的待選圖片池中，確定特徵值落入所述取值範圍內的待選圖片，作為與所述基準圖片對應的混淆圖片。

【第35項】

如申請專利範圍第34項所述的裝置，其中，所述取值範圍的最大值與所述基準圖片的特徵值的差值不大於預設的最大值，所述取值範圍的最小值與所述基準圖片的特徵值的差值不小於預設的最小值，所述特徵值不在所述取值範圍內。

【第36項】

如申請專利範圍第30項所述的裝置，其中，所述生成模組，在生成所述安全問題之前，將所述基準圖片進行模糊處理，作為所述基準圖片的副本，向所述終端發送刪除所述基準圖片的指令，並在本地保存所述基準圖片以及所述基準圖片的副本。

【第37項】

如申請專利範圍第30項所述的裝置，其中，所述測試保存模組，當所述答題結果與所述基準圖片匹配時，確定保存所述安全問題，當所述答題結果與所述基準圖片不匹配時，刪除所述安全問題。

【第38項】

如申請專利範圍第37項所述的裝置，其中，所述測試保存模組，向所述終端發送是否保存所述安全問題的詢問資訊，當所述終端返回保存所述安全問題的資訊時，保存所述安全問題，當所述終端返回不保存所述安全問題的資訊時，刪除所述安全問題。

【第39項】

如申請專利範圍第30項所述的裝置，其中，所述通訊

模組，向所述終端發送安全問題的生成指令以及若干待選圖片，接收所述終端根據所述生成指令從所述若干待選圖片中選擇並返回的圖片，作為所述基準圖片。

【第40項】

一種安全問題的生成裝置，所述裝置包括：

接收模組，接收伺服器發送的安全問題的生成指令；

監測生成模組，監測用戶的操作，並根據監測到的所述操作生成基準圖片；

發送生成模組，向所述伺服器返回所述基準圖片，以使得所述伺服器根據所述基準圖片生成安全問題；

其中，所述接收模組還用以接收所述伺服器生成的所述安全問題；

其中，所述發送生成模組還用以向所述伺服器返回對所述安全問題的答題結果，以使得所述伺服器確定所述答題結果與所述基準圖片是否匹配。

【第41項】

如申請專利範圍第40項所述的裝置，其中，所述監測生成模組，監測用戶在指定區域的手勢操作，並將所述手勢操作生成的圖像作為生成的所述基準圖片，或者監測用戶的操作，將感測器採集的圖像作為生成的所述基準圖片。

【第42項】

如申請專利範圍第40項所述的裝置，其中，所述裝置還包括：

刪除模組，根據所述接收模組接收的所述伺服器發送的刪除所述基準圖片的指令，將本地保存的所述基準圖片刪除。

【第43項】

一種身份驗證的裝置，所述裝置包括：

確定模組，根據待驗證帳戶，確定用於生成與所述待驗證帳戶對應的安全問題的基準圖片；

生成模組，根據所述基準圖片以及與所述基準圖片對應的各混淆圖片，生成安全問題；

發送模組，向所述待驗證帳戶所在的終端發送所述安全問題；

驗證模組，接收所述終端返回的選擇結果，並根據所述選擇結果對所述待驗證帳戶進行身份驗證，接收所述終端返回的選擇結果，判斷所述選擇結果與所述基準圖片是否匹配。

【第44項】

如申請專利範圍第43項所述的裝置，其中，與所述待驗證帳戶對應的安全問題存在多個；

所述確定模組，在確定用於生成與所述待驗證帳戶對應的安全問題的基準圖片之前，從與所述待驗證帳戶對應的各安全問題的標識中，選擇基於基準圖片生成的安全問題的標識。

【第45項】

如申請專利範圍第44項所述的裝置，其中，所述確定

模組，採用以下至少一種方法，選擇基於基準圖片生成的安全問題的標識：

根據各安全問題的標識分別對應的有效期，選擇當前時刻處於有效期內的安全問題的標識；根據各安全問題的標識對應的冷卻期，選擇當前時刻不處於冷卻期內的安全問題的標識；根據各安全問題的標識對應的優先順序，選擇安全問題的標識。

【第46項】

如申請專利範圍第45項所述的裝置，其中，所述確定模組，在選擇當前時刻處於有效期內的安全問題的標識之後，延長選擇的所述安全問題的標識對應的有效期。

【第47項】

如申請專利範圍第45項所述的裝置，其中，所述確定模組，在選擇當前時刻不處於冷卻期內的安全問題的標識之後，設置選擇的所述安全問題的標識對應的冷卻期。

【第48項】

如申請專利範圍第45項所述的裝置，其中，所述確定模組，在選擇安全問題的標識之後，降低選擇的所述安全問題的標識對應的優先順序。

【第49項】

如申請專利範圍第45項所述的裝置，其中，對所述安全問題的標識初始設置的優先順序，隨所述安全問題的標識生成時間至當前時刻的時長增加而降低，直至降低到預設的基礎優先順序為止。

【第 50 項】

如申請專利範圍第 45 項所述的裝置，其中，所述確定模組，針對每一個安全問題的標識，以當前時刻該安全問題的標識對應的優先順序越高，選擇該安全問題的標識的機率越高的方式，選擇安全問題的標識。

【第 51 項】

如申請專利範圍第 43 項所述的裝置，其中，所述驗證模組，當所述選擇結果與所述基準圖片匹配時，則確定所述待驗證帳戶的身份驗證結果為通過，當所述選擇結果與所述基準圖片不匹配時，則確定所述待驗證帳戶的身份驗證結果為不通過。

【第 52 項】

如申請專利範圍第 43 項所述的裝置，其中，所述待驗證帳戶為執行支付操作的帳戶；

所述驗證模組，根據所述選擇結果，對所述待驗證帳戶進行身份驗證，當所述身份驗證結果通過時，執行所述支付操作，當所述身份驗證結果不通過時，拒絕所述支付操作。

【第 53 項】

一種安全問題的管理裝置，所述裝置包括：

第一確定模組，確定帳戶對應的各安全問題；

第二確定模組，確定各安全問題分別對應的生成時間以及使用記錄；

第三確定模組，根據各安全問題對應的生成時間以及

使用記錄，確定各安全問題分別對應的有效期、優先順序以及冷卻期中的至少一種；

驗證選擇模組，當對所述帳戶進行身份驗證時，根據各安全問題分別對應的有效期、冷卻期以及優先順序中的至少一種，從所述帳戶對應的各安全問題中，選擇用於身份驗證的安全問題對所述帳戶進行身份驗證。

【第 54 項】

如申請專利範圍第 53 項所述的裝置，其中，所述第三確定模組，針對每個安全問題，根據該安全問題的生成時間至當前時刻的時長，確定當前時刻該安全問題的優先順序，其中，對該安全問題的優先順序，隨該安全問題生成時間至當前時刻的時長增加而降低，直至降低到預設的基礎優先順序為止。

【第 55 項】

如申請專利範圍第 53 項所述的裝置，其中，所述第三確定模組，針對每個安全問題，根據該安全問題對應的使用記錄，每使用一次該安全問題，延長一次該安全問題對應的有效期。

【第 56 項】

如申請專利範圍第 53 項所述的裝置，其中，所述第三確定模組，針對每個安全問題，根據該安全問題對應的使用記錄，每使用一次該安全問題，為該安全問題設置一個冷卻期。

【第 57 項】

如申請專利範圍第53項所述的裝置，其中，驗證選擇模組，根據所述帳戶對應的各安全問題分別對應的有效期、優先順序以及冷卻期，採用以下至少一種方法，從所述帳戶對應的各安全問題中，選擇用於身份驗證的安全問題：

根據各安全問題分別對應的有效期，確定當前時刻處於有效期內的安全問題；根據各安全問題對應的冷卻期，確定當前時刻不處於冷卻期內的安全問題；根據各安全問題對應的優先順序，以當前時刻該安全問題對應的優先順序越高，選擇該安全問題的機率越高的方式，選擇安全問題。

【第58項】

如申請專利範圍第57項所述的裝置，其中，所述驗證選擇模組，當確定所述安全問題不處於有效期內時，刪除所述安全問題以及所述安全問題對應的安全問題。