

Винахід стосується способу ідентифікації носія інформації і, зокрема, хоча й не виключно, зчитування кодів, які зберігаються в елементі безпеки, прикріпленому до карти або документа, як постійна послідовність магнітних властивостей, що виявляються, наприклад, таких, як зміна залишкової намагніченості уздовж елемента.

Носій інформації цього типу, як показано в GB-A-1,331,604, у якому у визначених областях елементарні анізотропні магнітні частки розсіяні і фіксовано виставлені в лінію уздовж попередньо встановленого напрямку, у той час як в інших областях частки не виставлені таким чином, або виставлені в лінію уздовж іншого попередньо встановленого напрямку. Це впорядкування звичайно описується як магнітний "водяний знак" або, як формування "постійної магнітної структури", тому що, на відміну від звичайних магнітних записів, тип залишкового намагнічування, обумовлений одноосовим магнетизмом чи "прояв" документа, може бути відновлений перенамагнічуванням, навіть після стирання, наприклад, за допомогою застосування альтернативного даному полю стирання. Магнітний "водяний знак" особливо добре підходить для запису даних у цифровій формі, тому що кожний розташований напрямок може бути визначений різним значенням, наприклад, двійковою "одиницею" або двійковим "нулем".

Завдяки "вбудованій" природі запису, елемент безпеки може бути зручно підготовлений як одиночна стрічка з "водяним знаком", яка містить рядки з двійковими закодованими числами (звичайно згрупованими в символи), що забезпечують властивість безпеки при відриві від стрічки і використовуються для забезпечення формування документа, або карти. Як правило, кожний рядок чисел відділений маркером, або "wartовим", що включає в себе унікальну послідовність бітів, яка сама ніколи не з'являється в секретній інформації. З цієї причини "wartовий" завжди може бути ідентифікований так, що біти, обрані для представлення секретної інформації (наприклад, набір символів, який з'являється в документі) можуть завжди бути відновлені за допомогою посилання на їхню позицію в документі.

Проте через проблеми допуску під час виробництва стрічки й проблеми сполучення між стрічкою й опорною стійкою, не можна, без використання дорогого устаткування, забезпечити появу "wartового" або "wartових" завжди в тому ж самому місці документа.

На практиці, коли один "wartовий" з'являється в кожному кінці документа, біти, обрані між "wartовими", представляють секретну інформацію. Проте, іноді, трапляється, що тільки один "wartовий" з'являється в документі, тому, залежно від точного положення, відповідна кількість бітів, обраних з обох кінців "wartового", береться для представлення секретної інформації, що ідентифікує цей документ. Таким чином, для кожної позиції першого виявленого "wartового" існують різні правила вибору бітів для вибору бітового представлення безпечних даних. Послідовність бітів, що представляє безпечні дані, може потім бути використана як перевірна інформація, або може бути використана для одержання перевіркою інформації, що, наприклад, користувач повинен надати перед тим, як карта перевіряється на правильність.

Технологія, проте, має слабкості, у випадках, коли перший "wartовий" на карті знаходиться близько до її краю. У цьому випадку можливо, що зчитувачу карти не вдасться виявити першого "wartового" і, замість цього, зчитається другий "wartовий" на карті. Таким чином, завжди існує можливість двозначності. Наприклад, уявимо, що карта, зроблена на фабриці, й частина магнітної стрічки прикріплена до карти, стрічка має номер 300 разом із частинами з номерами 299 і 301. Карта прочитана на фабриці і їй привласнений ідентифікаційний номер 300. Не знаючи як "wartові" розташовані стосовно краю карти, зчитувачі карти можуть у полі розпізнати ідентифікаційний номер карти як 299, 300, або 301. Це, зрозуміло, небажано для карт, використовуваних у фінансових транзакціях, тому що це могло б, можливо, сплутати дві карти, що мають примикаючи частини стрічок із "водяними знаками", прикріпленими до них. Це також небажано для карт, використовуваних при страхових позовах, або дозволу доступу, або посвідчень, або тих, які мають деяку цінність, такі, як попередньо оплачені проїзні карти.

З метою вирішення цієї проблеми стрічка з "водяним знаком", виготовлена компанією THORN Security Science Ltd, Swindon, England, часто прикріплюється до карт точно підігнаною так, що "wartові" завжди зустрічаються в тому ж самому місці на карті. Збільшення витрат виробництва зв'язано з такими позначеними картами. Альтернативне рішення, описане в GB-A-2,021,835, стирає запис позиції маркера в документі.

Згідно з винаходом, наданий спосіб ідентифікації носія інформації, відповідно до формули винаходу. Це може забезпечити перевагу ідентифікації унікального носія інформації без звертання до дорогих схем припасування для забезпечення того, щоб маркери завжди знаходилися на тих самих місцях на носії інформації.

Для гарантування того, що носій інформації буде однозначно ідентифікований, необхідно, щоб кожне раціональне число в послідовності не було б повторене і різниця між числами, що йдуть один за одним, повинна дорівнювати, або бути більше, ніж одиниця. На практиці, достатньо мати досить довгу послідовність так, щоб при використанні карта або документ застарівали до того, як послідовність почне повторюватися. Маркери, які йдуть один за одним, найбільш зручно упорядковувати з переміщенням в одному заданому напрямку. Переважно, щоб маркери, які йдуть один за одним, однаково відстояли друг від друга.

Переважно, щоб носій інформації, який включає документ або карту, містив би елемент безпеки, що має дані закодовані на ньому у виді постійної кодограми з магнітними властивостями, що виявляються, а фіксована точка на носії інформації визначалася б краєм документа або карти. Це спрощує вимір відстані в частині а) вищезгаданого способу.

Реалізації даного винаходу будуть тут описані, тільки на прикладі, із посиланням на креслення, на яких: фіг. 1 показує довжину стрічки, закодованої магнітним способом, яка містить безпечний елемент; фіг. 2 показує носій інформації у вигляді карти, і фіг. 3 показує блок-схему способу згідно з винаходом.

На фіг. 1 показаний схематично відрізок стрічки з "водяним знаком" (10) фірми Thorn Secure Science Ltd, Swindon, England. Стрічка має постійно намагнічену структуру. Закодовані дані уміщують маркери, відомі, як стартові "wartові" (11), що мають ідентифікаційні номери (12, 13, 14) у вигляді двійкових розрядів. Ідентифікаційні номери в послідовності являють собою цілі упорядковані по зростанню величини, наприклад, 300, 301, 302, 303 і так далі.

Фіг. 2 показує частину стрічки з фіг. 1, прикріплену до кредитної карти 15. Відстань між краєм карти 16 і початком першого маркера, або початком "wartового" (x) позначена на фіг. 2 за допомогою виноски під номером 17. Відстань між краєм карти 16 і початком другого маркера або початком wartового позначена на фіг. 2 за допомогою виноски під номером 18.

Винахідники установили, що шляхом обробки ідентифікаційного номера не у вигляді послідовності цілих чисел, а у вигляді безперервно мінливої кількості, можна виключити двозначність, властиву для інших способів ідентифікації частин стрічки, що примикають.

Вважається, що кожний ідентифікаційний номер починається на початку маркера, або на початку "wartового", зліва від ідентифікаційного номера на фіг. 2. Тому, початок старту "wartового" перед ідентифікаційним номером N, аналогічний позиції N 000 (наприклад, 0.000, якщо N=0). Вимірник включає зчитувальну магнітну голівку, що шукає перший маркер, або початок "wartового".

Вимірник міряє відстані (x, 17) між краєм карти 16 і початком першого маркера, а також зчитує число, яке слідує за маркером. Ця аналогова відстань потім виражається часткою кроку маркера, за рахунок ділення x на відстань між маркерами (наприклад, 18-17).

Ця частка, звичайно, обчислюється безпосередньо. Дані на карті, звичайно, набираються з постійним кроком і встановлюється самосинхронізація. Наприклад, дані з "водяним знаком" звичайно кодуються з постійним кроком 33 біта на дюйм, і можуть у реалізації мати 70 бітів між початком "wartових", що йдуть один за одним. Підраховуючи кількість бітів, отриманих до першого розпізнаного початкового "wartового", і ділячи на 70, одержуємо відстань між краєм карти і першим початковим "wartовим", виражене дробом між 0 і 1. Наприклад, якщо 22 біта отримані до першого початкового "wartового", одержуємо $22/70=0,31$. Тому, якщо наступне число дорівнює N, то відповідний ідентифікаційний буде дорівнювати числу N мінус 0,31.

Якщо декодування почалося з другого початкового "wartового" замість першого, то число бітів до цього початкового "wartового" буде дорівнювати 92. Таким чином, x буде дорівнювати $92/70=1,31$. Декодоване число, яке слідує за початковим "wartовим" у цьому випадку N+1, і, тому, віднімаючи його з N+1 одержуємо N мінус 0,31, як і раніше. Очевидно, що в цьому випадку, спосіб буде працювати, якщо до одиниці додати 1-x замість вирахування x. Спосіб також буде працювати, якщо додати x, але тільки, якщо послідовність представляє цілі величини, що зменшуються, (наприклад, при читанні карти у протилежному напрямку й виміру від іншого кінця карти).

Хоча кінець числа, відзначеного, як 14 на фіг. 2, відсутній на карті 15, він може бути реконструйований відповідним алгоритмом, який працює з доступною частиною 14 і останньою частиною 13, що передують початковому "wartовому".

Реалізація способу згідно з винаходом показана блок-схемою на фіг. 3. На цьому малюнку блоки мають такі значення.

Блок 1 позначає вимір відстані від фіксованої точки на носії інформації до даної частини маркера, блок 2 позначає ділення цієї відстані на відстань між відповідними заданими частинами маркерів, що йдуть один за одним, за допомогою чого одержують раціональне число (x), і блок 3 позначає додавання або вирахування цього раціонального числа (x) до (із) числа з послідовності, суміжної з вищезгаданим маркером, у даному напрямку, за допомогою чого одержують таке раціональне число, що дозволяє однозначно ідентифікувати носій інформації.

На закінчення відзначимо, що зміст пріоритетного документу для даної заявки (зокрема, малюнків і реферату) приведено тут у якості довідкового матеріалу.

35650

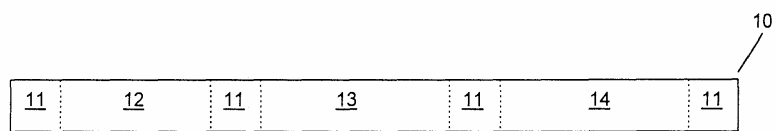


Fig. 1

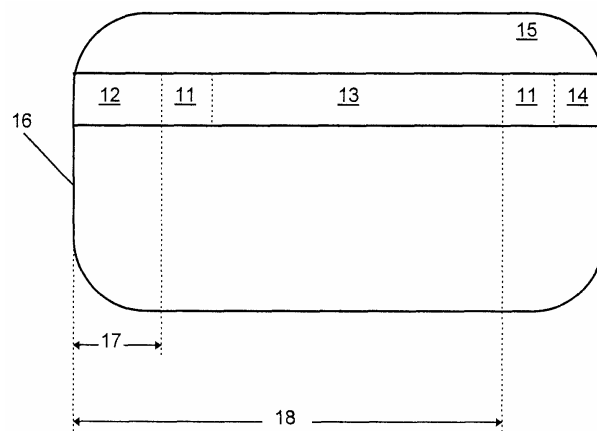


Fig. 2

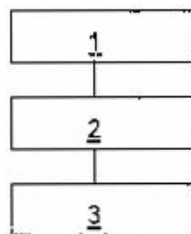


Fig. 3