US 20110186397A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2011/0186397 A1

(43) Pub. Date: Aug. 4, 2011

SHEIKH

(54) **SUITCASE WITH BIOMETRIC LOCK MECHANISM**

(75) Inventor: **HAROON SHEIKH**, Miami, FL (US)

(73) Assignee: **Heys (USA), Inc.**, Weston, FL (US)

(21) Appl. No.: **12/986,889**

(22) Filed: **Jan. 7, 2011**

Related U.S. Application Data

(60) Provisional application No. 61/299,699, filed on Jan. 29, 2010.

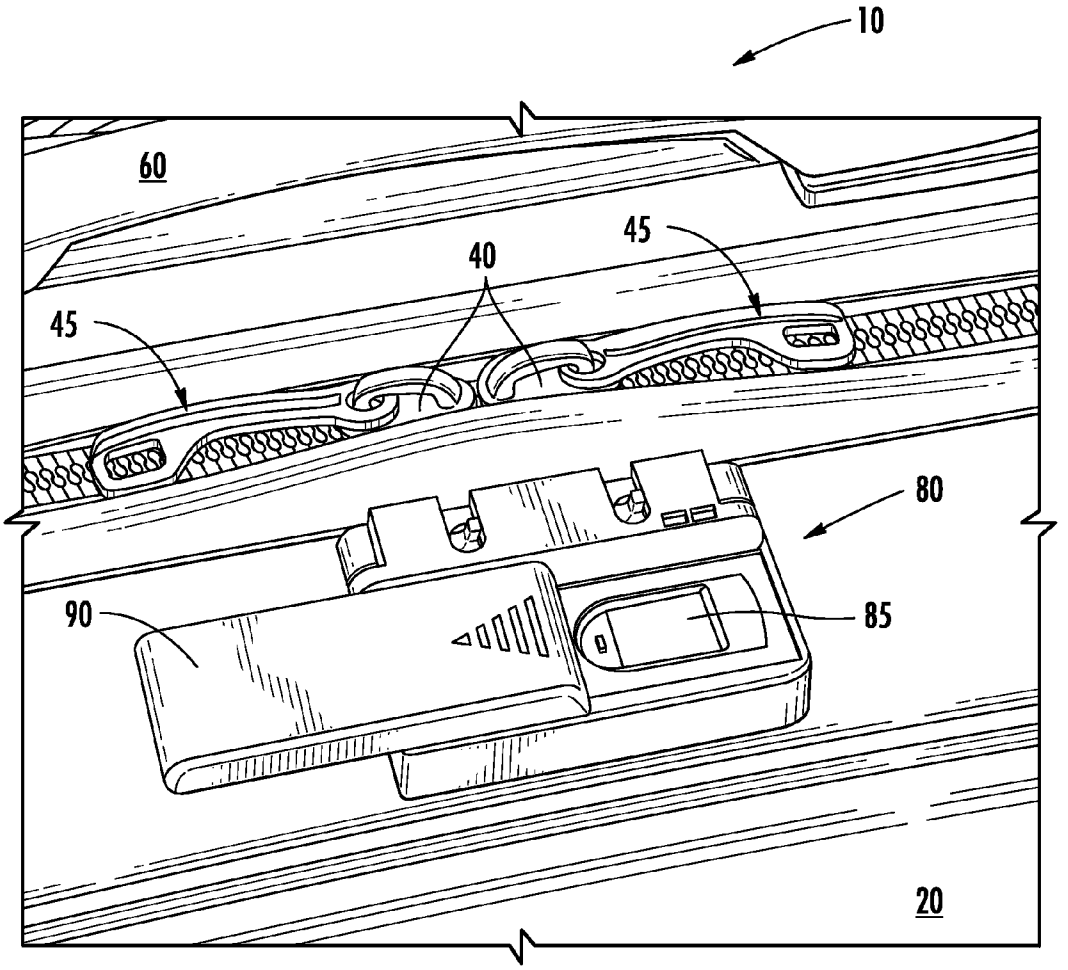
Publication Classification

(51) **Int. Cl.**
A45C 13/00 (2006.01)

(52) **U.S. Cl.** **190/120**

(57) **ABSTRACT**

A suitcase featuring a biometric lock may be provided. The suitcase may include a plurality of hard-sided shells for forming storage compartments of the suitcase. Additionally the suitcase may include a fastening mechanism for connecting the plurality of hard-sided shells. The fastening mechanism may be utilized to provide access to at least one storage compartment of the storage compartments. The biometric lock of the suitcase may be configured to prevent unauthorized access to one or more storage compartments of the suitcase. The biometric lock may include a memory device configured to store a plurality of fingerprints. Also, the biometric lock may include a biometric reader, which may be configured to receive a fingerprint from a user. The biometric reader may be further configured to unlock the biometric lock when a received fingerprint matches a stored fingerprint of the plurality of stored fingerprints.



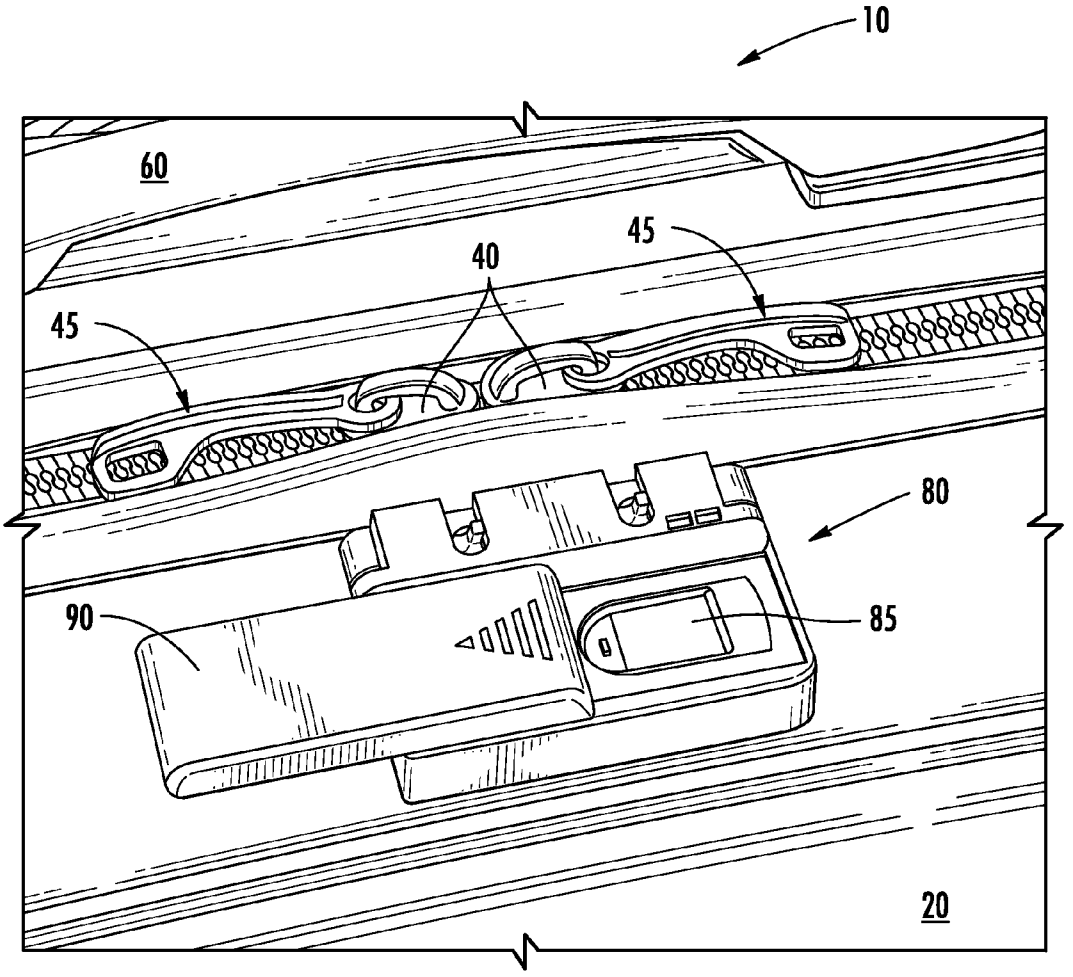


FIG. 1

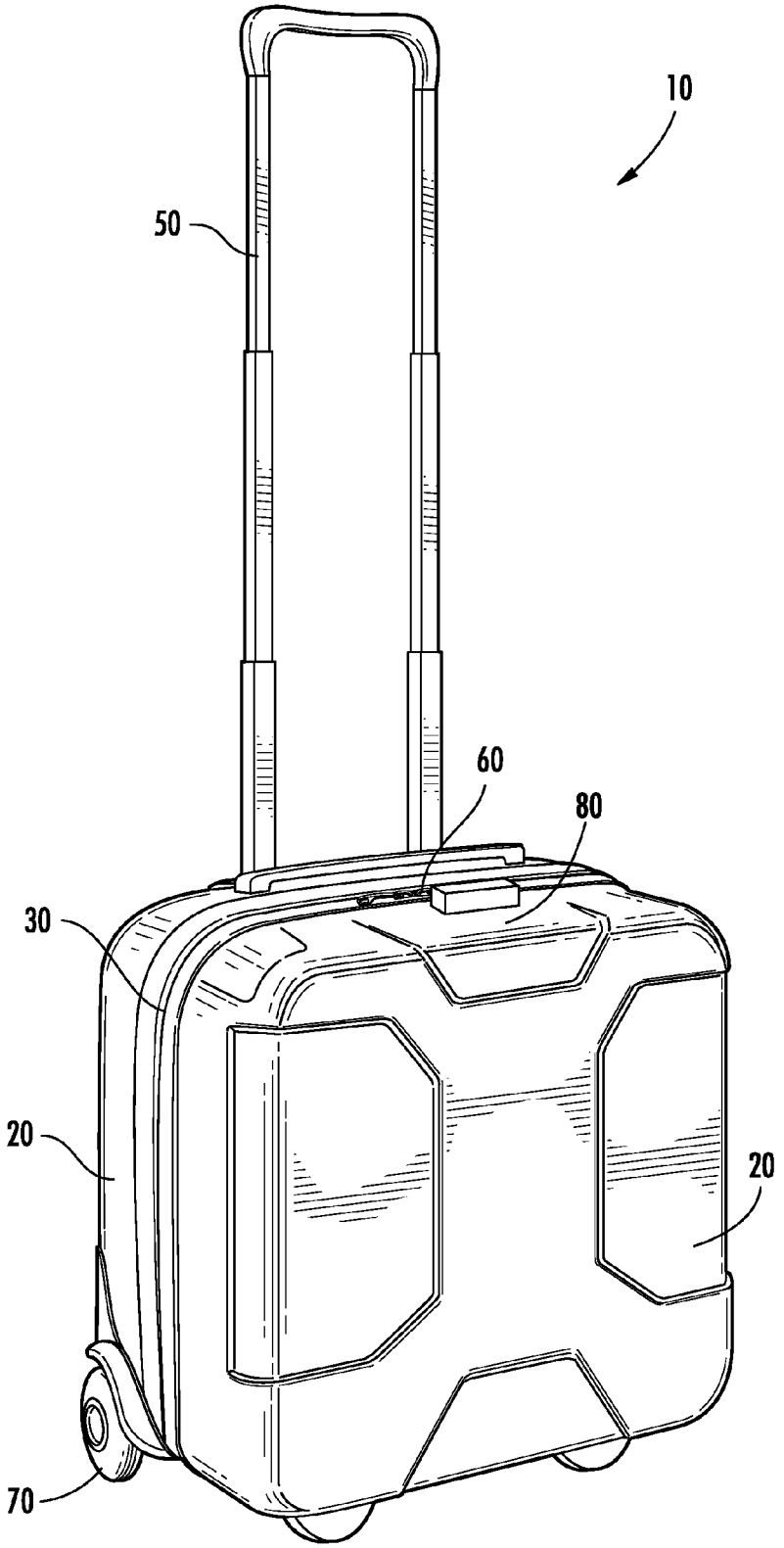


FIG. 2

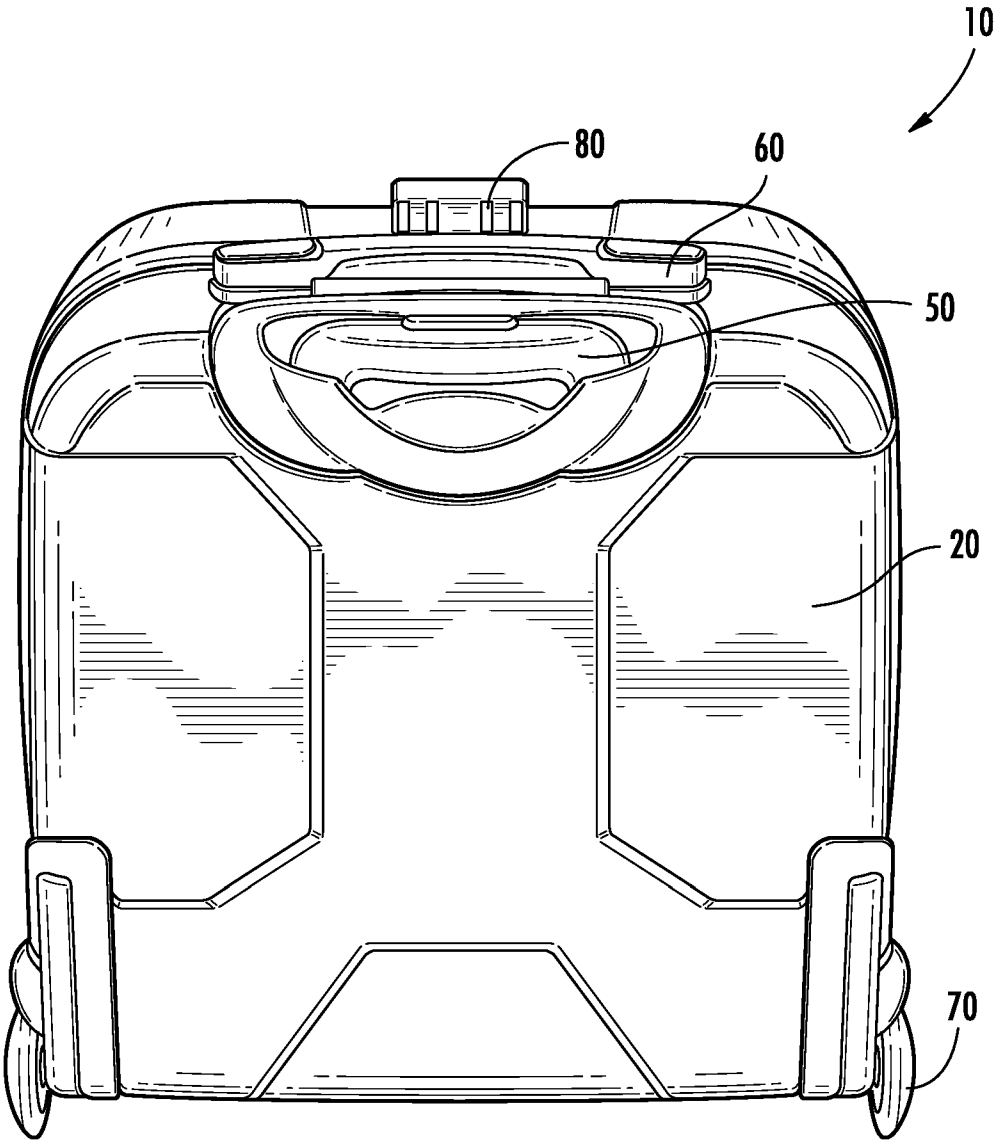


FIG. 3

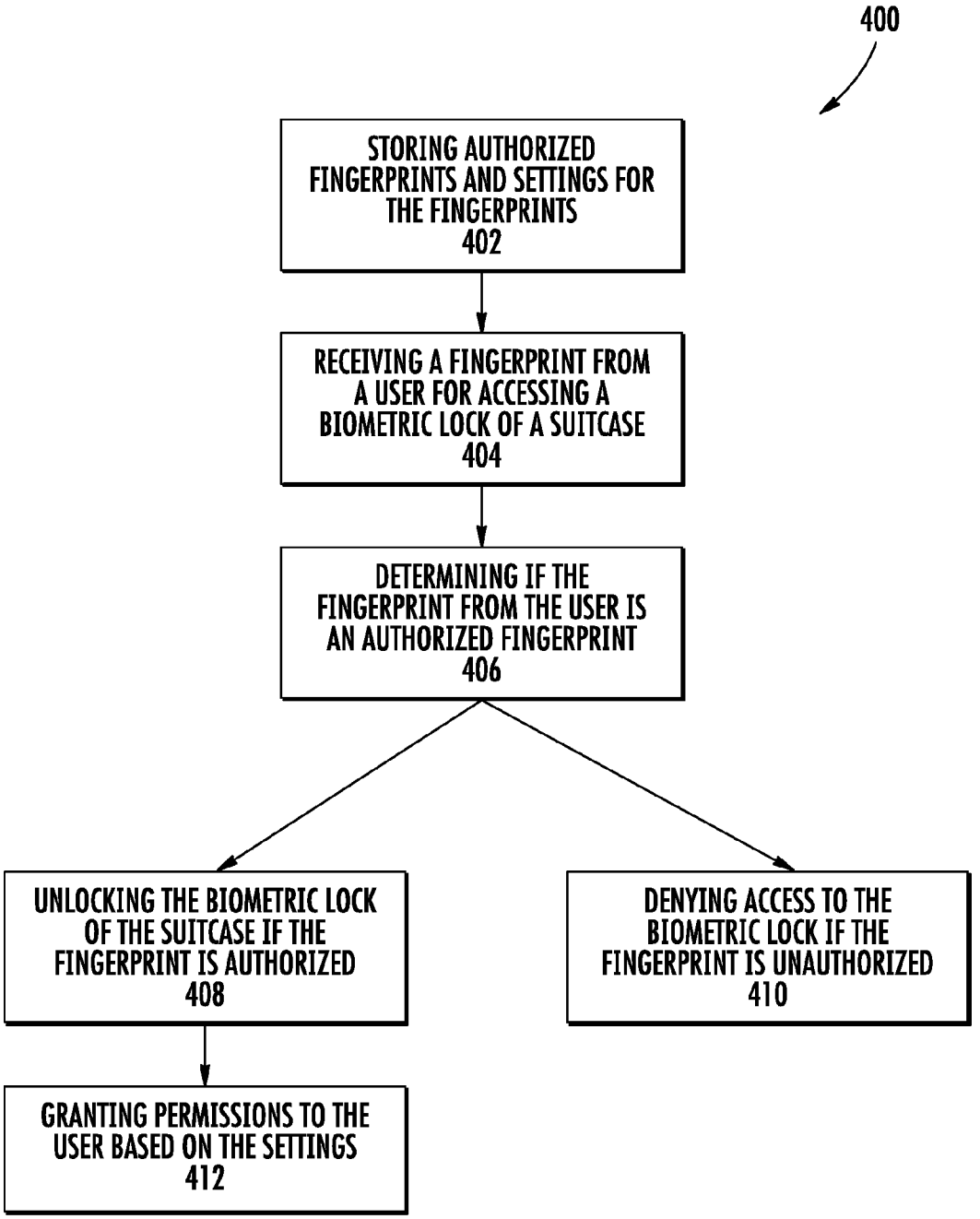

400
STORING AUTHORIZED FINGERPRINTS AND SETTINGS FOR THE FINGERPRINTS
402
RECEIVING A FINGERPRINT FROM A USER FOR ACCESSING A BIOMETRIC LOCK OF A SUITCASE
404
DETERMINING IF THE FINGERPRINT FROM THE USER IS AN AUTHORIZED FINGERPRINT
406
UNLOCKING THE BIOMETRIC LOCK OF THE SUITCASE IF THE FINGERPRINT IS AUTHORIZED
408
DENYING ACCESS TO THE BIOMETRIC LOCK IF THE FINGERPRINT IS UNAUTHORIZED
410
GRANTING PERMISSIONS TO THE USER BASED ON THE SETTINGS
412

FIG. 4

SUITCASE WITH BIOMETRIC LOCK MECHANISM

RELATED APPLICATIONS AND PRIORITY

[0001] The present application claims priority to U.S. Provisional Application No. 61/299,699, filed Jan. 29, 2010, the entirety of which is hereby incorporated by reference.

FIELD OF THE INVENTION

[0002] The present application relates to luggage, and more particularly to a suitcase which features a biometric lock mechanism.

BACKGROUND

[0003] Currently, consumers have a variety of different options when it comes to storing their personal belongings and/or other articles. For example, consumers can use suitcases, briefcases, computer cases, beauty cases, business cases, travel bags, and a host of other types of cases. People often spend considerable resources to ensure that they have suitcases which are both durable and stylish. However, most importantly people put significant importance on having a suitcase which effectively secures their belongings, while also being highly resistant to tampering. Accordingly, many suitcases come with combination locks, latch mechanisms, or other similar mechanisms so as to ensure that others cannot easily access their belongings, which can often have tremendous value or are often times irreplaceable. Current mechanisms provide some level of security to consumers, however, they are often times not as effective as consumers would desire.

SUMMARY

[0004] The present disclosure relates to a suitcase including security features for preventing unauthorized access to the suitcase. The suitcase may be hard-sided, soft-sided, or a combination thereof. The suitcase may include a biometric lock, which may be configured to scan physical identifiers, such as, but not limited to, fingerprints, irises, faces, blood, and handprints of various users attempting to access the suitcase. The biometric lock may include a biometric reader, which may be configured to analyze the physical identifiers of the users and determine if the physical identifiers have been previously authorized to access one or more storage compartments of the suitcase. If the analysis performed by the biometric reader indicates that the physical identifier was not authorized, the user may be denied access to the suitcase. On the other hand, if the analysis indicates that the physical identifier was authorized, the user may be granted access to the suitcase.

[0005] According to one aspect of the exemplary embodiments of the present disclosure, a hard-sided suitcase may be provided. The hard-sided suitcase may include at least two hard-sided shells. The hard-sided shells may be utilized to form one or more storage compartments of the hard-sided suitcase. Additionally, the hard-sided suitcase may include a zipper mechanism, which may be utilized to connect the hard-sided shells together and to provide access to the storage compartments of the hard-sided suitcase. The hard-sided suitcase may further include a biometric lock, which may be attached to a portion of the at least two hard-sided shells and which may be configured to lock the zipper mechanism. The biometric lock may be utilized to prevent unauthorized access to one or more storage compartments of the hard-sided suitcase. Notably, the biometric lock may include a memory device configured to store at least one authorized fingerprint for accessing the suitcase. Also, the biometric lock may include a fingerprint reader, which may be configured to unlock the biometric lock when an authorized fingerprint of the at least one authorized fingerprint is received by the fingerprint reader. Upon unlocking the biometric lock access may be provided to the zipper mechanism so as to provide access to the at least one storage compartment of the suitcase.

[0006] In another aspect according to the exemplary embodiments, a suitcase may be provided. The suitcase may include a plurality of shells for forming storage compartments of the suitcase. The plurality of shells of the suitcase may comprise at least two hard-sided shells. The suitcase may also include a zipper mechanism for connecting the plurality of shells, wherein the zipper mechanism may be utilized to provide access to at least one storage compartment of the storage compartments. Furthermore, the suitcase may include a biometric lock configured to prevent unauthorized access to the at least one storage compartment of the storage compartments. The biometric lock may include a memory device configured to store a plurality of fingerprints. The biometric lock may further include a biometric reader, which may be configured to receive a fingerprint, wherein the biometric reader is configured to determine if the received fingerprint matches a stored fingerprint of the plurality of stored fingerprints. When the received fingerprint matches the stored fingerprint, the biometric reader may be configured to provide access to the zipper mechanism of the suitcase.

[0007] In another aspect, a suitcase may be provided. The suitcase may include a plurality of hard-sided shells utilized to form storage compartments of the suitcase. Additionally, the suitcase may include a fastening mechanism for connecting the plurality of hard-sided shells. The fastening mechanism may be utilized to provide access to at least one storage compartment of the storage compartments of the suitcase. The suitcase may further include a biometric lock, which may be configured to prevent unauthorized to the at least one storage compartment of the storage compartments. The biometric lock may include a memory device configured to store a plurality of physical identifiers and the biometric lock may include a biometric reader. Notably, the biometric reader may be configured to receive a physical identifier and to unlock the biometric lock when the received physical identifier matches a stored physical identifier of the plurality of stored physical identifiers.

[0008] Further details are provided in the following description of the embodiments of the present disclosure, which have been shown and described by way of illustrations. As will be realized, other and different embodiments are possible, and its details are capable of modification in various respects. Accordingly, the drawings and description are illustrative in nature and not restrictive.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] There are shown in the drawings arrangements which are presently discussed, it being understood, however, that the invention is not limited to the precise arrangements and instrumentalities shown, wherein:

[0010] FIG. **1** illustrates a portion of an exemplary hard-sided suitcase featuring a biometric lock mechanism according to an embodiment of the invention.

[0011] FIG. **2** illustrates an exemplary view of the hard-sided suitcase featuring the biometric lock mechanism of FIG. **1**.

[0012] FIG. **3** illustrates a back view of the hard-sided suitcase featuring the biometric lock mechanism of FIG. **1**.

[0013] FIG. **4** illustrates an exemplary method for accessing a suitcase featuring a biometric lock mechanism according to an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0014] The exemplary embodiments of the disclosed herein are described with respect to a suitcase for carrying and/or storing different types of articles. More specifically, the present disclosure discloses a suitcase including a biometric lock for preventing unauthorized access to the suitcase. It should be understood by one of ordinary skill in the art that the exemplary embodiments of the present disclosure can be applied to other types of suitcases. The term "suitcase" as used herein is intended to encompass a variety of different types of luggage. For example, the suitcase may be, but is not limited to being, a traditional suitcase, a briefcase, a laptop bag/case, a computer bag/case, a business case, a travel bag, a beauty case, or various other types of luggage. Notably, the aforementioned types of suitcases are merely listed for illustrative purposes and are not intended to limit the suitcase to the listed varieties.

[0015] According to one embodiment, a hard-sided suitcase may be provided. The hard-sided suitcase may include at least two hard-sided shells. The hard-sided shells may be utilized to form one or more storage compartments of the hard-sided suitcase. Additionally, the hard-sided suitcase may include a zipper mechanism, which may be utilized to connect the hard-sided shells together and to provide access to the storage compartments of the hard-sided suitcase. The hard-sided suitcase may further include a biometric lock, which may be attached to a portion of the at least two hard-sided shells and which may be configured to lock the zipper mechanism. The biometric lock may be utilized to prevent unauthorized access to one or more storage compartments of the hard-sided suitcase. Notably, the biometric lock may include a memory device configured to store at least one authorized fingerprint for accessing the suitcase. Also, the biometric lock may include a fingerprint reader, which may be configured to unlock the biometric lock when an authorized fingerprint of the at least one authorized fingerprint is received by the fingerprint reader. Upon unlocking the biometric lock access may be provided to the zipper mechanism so as to provide access to the at least one storage compartment of the suitcase.

[0016] Referring to the drawings, an embodiment of a suitcase **10** for preventing unauthorized access to the suitcase **10** is illustrated. The suitcase **10** may include front, back, side, and top and bottom portions. The suitcase **10** may include at least two shells **20**, which may be utilized to form one or more storage compartments for the suitcase **10**. The shells **20** may be either hard-sided shells and/or soft-sided shells. Hard-sided shells may include, but are not limited to including, a thermoplastic composition, polycarbonate, a polycarbonate composite, acrylonitrile butadiene styrene (ABS), polypropylene, plastic, wood, and/or metal. In an embodiment, the shells **20** can be comprised of a polycarbonate composition, which can include adding one or more other substances to the composition, such as ABS plastic and the like to the composition. The polycarbonate composition may be lightweight and may enable the shells **20** to be flexible, while maintaining a generally rigid form. When stressors are applied to the shells **20**, the polycarbonate composition may allow the shells **20** to absorb the impact from the stressors and cause the shells **20** to flex to accommodate the stressors. After the stressors have been removed, the polycarbonate composition may enable the suitcase **10** to return to its original shape. Soft-sided shells may include, but are not limited to, polyester, nylon, fabric, a fabric combination, wool, linen, leather, and/or other soft-sided luggage materials.

[0017] Outer portions of the shells **20** may form at least a portion of the front, back, sides, top and bottom portions of the suitcase **10**. The inner portions of the shells **20** may be lined with various types of fabrics or other similar features and may include one or more pockets, which can be opened and closed through zipper mechanisms or other mechanisms for opening and closing pockets. The pockets may vary in height, length, and width and may be tailored to store specific types of personal articles. A suitable lining material may be nylon, although any other materials may be utilized as well. In an embodiment, two of the shells **20** may be utilized to form a primary compartment of the suitcase **10**. The primary compartment may be utilized by a user to store the bulk of a user's storage items. One or more other shells **20** may be utilized to form one or more secondary compartments as well. Secondary compartments may be utilized to store smaller items or store specific types of items.

[0018] The shells **20** can be connectable to one another through the use of a zipper **30** or other fastening mechanism such as, but not limited to, snap fasteners, buttons, ties, and buckles. The zipper **30** may be utilized to provide access to one or more storage compartments of the suitcase **10**. Each side of the zipper **30** may include a plurality of metal or plastic teeth, which may be stitched or otherwise attached to corresponding pieces of fabric tape. The fabric tape may be comprised of ballistic nylon or other similar materials. One fabric tape may be stitched or otherwise fastened to an edge of one of the shells **20** and the other fabric tape may be fastened to an edge of another shell **20**. The zipper **30** may include one or more sliders **40**, which may be configured to hold at least a portion of the plurality of teeth on each side of the zipper **30**. Once a slider **40** is slid across the plurality of teeth, it may be utilized to connect the edges of the shells **20** together, which forms a seal for the storage compartments within the shells **20**.

[0019] Additionally, the zipper **30** may include one or more pull tabs **45**. The pull tabs **45** may be attached to the zipper **30** via openings in the sliders **40**. A user may pull the pull tabs **45** to slide the sliders **40** of the zipper **30** across the plurality of teeth of the zipper **30**. The pull tabs **45** may be utilized to separate a pair of sliders **40** from each other and thereby open the zipper **30**. Also, the pull tabs **45** may be utilized to bring a pair of sliders **40** together so as to close the zipper **30**. In one embodiment, the zipper **30** may be slid across the entire edges of the hard-sided shells. Such a configuration would allow the compartments to be entirely or almost entirely separated upon completely unzipping the edges from one another. However, in another embodiment, the suitcase may have a hinge, preferably along the bottom portion of the suitcase. The hinge may permanently connect at least a portion (such as the bottom portion) of the edges of the hard-sided shells together. The remaining portions of the edges that are not connected by the hinge may be connectable via the zipper mechanism **30**.

By utilizing the hinge, this may allow the shells **20** to remain at least partially connected to one another, particularly in the event that the zipper **30** fails.

[0020] Additionally, the suitcase **10** may include one or more handles for carrying, pulling, pushing, and/or lifting the suitcase. The handles may include a telescoping handle **50**. The telescoping handle **50** can be connected to a top portion or other portion of a shell **20** so as to allow for easy transportation of the suitcase. The telescoping handle **50** may be operated by utilized a lock button. The handle **50** may include trolley tubes, which may extend through a portion of the shell **20** to which it is attached. This may allow for additional structural support and may allow the handle to undergo a greater amount of stress. In an embodiment, the trolley tubes may be encased within a storage compartment into a protrusion along the backside of the shell **20**. In an embodiment, the encasing may be performed by laying a fabric, plastic, or other material across the trolley tubes so as to ensure a flat surface. Once the trolley tubes are encased, a flat surface can be created across the trolley tubes. This allows one to pack the compartment of the suitcase without having to pack around the trolley tubes, while also ensuring a more uniform compartment space. It should be noted that the trolley tubes do not necessarily have to be encased and that other configurations are contemplated. In addition to the telescoping handle **50**, one or more carry handles **60** may also be provided. For example, one carry handle **60** may be provided on each of the top and side of the suitcase **10** on a large suitcase, whereas only one carry handle **60** may be sufficient on the top of a smaller suitcase **10**, such as a briefcase.

[0021] The suitcase **10** may also be configured to include a plurality of wheels **70** for transporting the suitcase. Each wheel **70** may include a hub portion and a rubber portion which surrounds the hub portion. The hub portion of each wheel **70** may be affixed to the suitcase **10**, while also allowing each wheel **70** to spin when the suitcase **10** is rolled by a user. In one configuration, two wheels **70** may be connected to a bottom portion of a shell **20**, preferably along the opposite ends of the bottom of the shell **20**. In another configuration, another set of wheels **70** may be connected to a bottom portion of another shell **20** so as to allow for four wheels **70** positioned at the four ends of the bottom of the suitcase **10**. Any number of wheels **70** and any position for placement of the wheels **70** may be utilized as well. For example, one wheel **70** may be placed on a bottom portion of one shell **20** and two wheels **70** may be placed on a bottom portion of another shell **20**. Such a positioning may allow for greater stability and for easier transportation of the suitcase **10**. In one embodiment, the hub portions of the wheels **70** may be plated with chrome or another similar material. Plating the hub portions of the wheels **70** with chrome or other similar materials may enable the wheels **70** to rotate along a variety of surfaces in a smooth and easy motion by minimizing friction and drag along the surfaces.

[0022] Furthermore, the suitcase **10** may be configured to have one or more expandable portions, which may be utilized to expand one or more storage compartments of the suitcase **10**. An expandable portion may be connected to at least one of the shells **20** either at an edge of the shell **20** or otherwise and may be made of fabric such as nylon or other materials which can expand to various different sizes. Notably, the expandable portion may be secured in a non-expanded state by utilizing a zipper **30** or other similar fastening mechanism. When an individual pulls a slider **40** to open the zipper **30** for the expandable portion, the expandable portion may expand so as to increase the storage capacity of the suitcase **10**. If the individual would like to return the suitcase **10** to its original size, the individual may close the zipper mechanism **30** using the sliders **40** and/or the pull tabs **45**.

[0023] In an embodiment, the suitcase **10** may include a locking mechanism for preventing unauthorized access to one or more compartments of the suitcase **10**. The locking mechanism may be a biometric lock **80**, which, for example, may be configured to read fingerprints or other physical identifiers such as, but not limited to, an iris, a handprint, palm print, blood, and faces. Placement of the biometric lock **80** may be along a top portion of at least one of the shells **20** and may be used to limit access to compartments of the suitcase **10**, however, the biometric lock **80** may be placed along other portions of the suitcase **10** as well. The biometric lock **80** may include a biometric reader **85** (e.g. fingerprint reader, iris scanner, facial recognition device, blood scanner, and hand scanner), a sliding cover **90** for concealing the biometric reader **85**, a memory device, and a power source for powering the biometric reader **85** and/or the biometric lock **80**. The memory device may be configured to store one or more fingerprints or other physical identifiers for multiple authorized users. For example, in one arrangement, eight fingerprints may be stored by the memory device. The fingerprints stored by the memory device may be designated as an administrator fingerprint or a non-administrator fingerprint In an embodiment, two administrator fingerprints and six non-administrator fingerprints may be stored.

[0024] An administrator and/or owner of the suitcase **10** may designate a fingerprint as an administrator fingerprint or a non-administrator fingerprint. Additionally, the administrator/owner of the suitcase **10** may set access rights and other configurable settings for each fingerprint stored in the memory device of the biometric lock **80**. Access rights and other configurable settings may include, but are not limited to including, a frequency at which a particular fingerprint can be utilized to access the biometric lock, an expiration date associated with a particular fingerprint, a time frame to access the biometric lock **80**, a time period for automatically locking the biometric lock **80** after access is provided to the zipper mechanism **30**, rankings associated with fingerprints, the ability to add or delete users/fingerprints, and administrator privileges. For example, an administrator may have full rights to the biometric lock **80** and may be able to access, lock, and unlock the biometric lock **80** at any time and may adjust settings associated with the biometric lock **80**. Non-administrator fingerprints, on the other hand, may be configured, but is not limited to being configured, to be used only one time, up to a threshold number of times, and/or at a particular designated time. Non-administrator users may also be prevented from adjusting any settings associated with the biometric lock **80**.

[0025] In an embodiment, the biometric lock **80** may be configured to be connectable to a computer by utilizing a universal serial bus device (USB). Such a USB device may include, but is not limited to including, Standard-A, Standard-B, mini-USB, and/or micro-USB devices. Fingerprints, data, and settings associated with the biometric lock **80** may be transferred from the biometric lock **80** to the computer via the USB device, which may be connected to the biometric lock **80** and the computer via USB ports. The fingerprints and settings that are transferred to the computer may be stored in a storage device, such as a hard drive, of the computer. Instead of

directly connecting the biometric lock **80** to a computer via a USB device, a portable USB device may also be utilized. The portable USB device may be connected to a USB port of the biometric lock **80** and the memory device of the biometric lock **80** may transfer fingerprints, settings, and/or other data to the portable USB device. Once the fingerprints, settings, and/or other data have been transferred to the portable USB device, the portable USB device may be connected to a computer and then transferred to a storage device of the computer. Settings, fingerprints, and/or other data may be managed and/or adjusted by an administrator or other user with administrator privileges via the computer as well.

[0026] In an embodiment, the sliding cover **90** for concealing the biometric reader **85** may be utilized to cover the biometric reader **85** when the biometric reader **85** is not in use. However, when a user is ready to use the biometric reader **85** and attempt to unlock the biometric lock **80**, the user may slide away or otherwise adjust the cover **90** to reveal the biometric reader **85** of the biometric lock **80**. The power source for the biometric lock **80** may be a battery or other power source and may, in an embodiment, be located within the suitcase **10**. However, the power source may also be located within the biometric lock **80** itself. By locating the power source of the lock within the biometric reader **85**, biometric lock **80**, or within the suitcase **10**, it may serve to prevent individuals from easily disabling the lock by removing the battery or other power source. The battery may be, but is not limited to being, a rechargeable lithium battery, a non-rechargeable lithium battery, an alkaline battery, a zinc-carbon battery, a nickel metal hydride battery, a nickel-zinc battery, and a nickel-cadmium battery. The battery may be configured to be charged in the suitcase **10** via one or more USB ports of the suitcase **10**. Notably, the battery may be configured to provide several months of power on a single charge.

[0027] Operatively, a user may slide away the sliding cover **90** in order to access the biometric reader **85** of the biometric lock **80**. When the user presses his or her finger on the biometric reader **85**, the biometric reader **85** may analyze the fingerprint of the user and determine if the fingerprint has been stored in the memory device. If the fingerprint is found to be in the memory device, the fingerprint may be an authorized fingerprint and the biometric lock **80** may open and provide the user with access to one or more storage compartments of the suitcase **10**. After the user is done using and/or packing the suitcase **10**, the user may lock the biometric lock **80**. If the fingerprint is not found to be in the memory device, the fingerprint may be an unauthorized fingerprint and the user may be denied access to the biometric lock **80** and, therefore, denied access to the compartments of the suitcase **10**.

[0028] In an embodiment, the biometric lock **80** may be configured to lock in one or more sliders **40** and/or one or more pull tabs **45** of the zipper **30**. In FIG. **1**, the biometric lock **80** is positioned on a location of the suitcase **10** to lock in the pull tabs **45** with relative ease. Another configuration may be utilized to lock in the sliders **40**. The sliders **40** and/or pull tabs **45** may have apertures at free ends thereof, which the biometric lock **80** may use to lock the sliders **40** and/or pull tabs **45** in an immovable position so as to prevent an unauthorized user from accessing the compartments of the suitcase **10**. When the biometric reader **85** detects that a fingerprint of a user matches an authorized fingerprint, the biometric lock **80** may be configured unlock the sliders **40** and/or the pull tabs **45** and allow the authorized user to open the zipper mechanism **30** using the unlocked sliders **40** and/or pull tabs **45**.

[0029] In an embodiment, the memory device of the biometric lock **80** may be configured to store any and all received fingerprints, even if they are unauthorized. Similarly, a computer may also store the fingerprints as well by using a USB device or other similar device. Unauthorized fingerprints may be stored in an unauthorized fingerprint list and authorized fingerprints may be stored in an authorized fingerprint list. If a user's fingerprint has been previously stored in the unauthorized fingerprint list and the user presses his or her finger on the biometric reader **85** again, the biometric lock may be configured to emit a warning signal. Additionally, even if the unauthorized fingerprint was not stored in an unauthorized fingerprint list, the biometric lock **80** may emit the warning signal whenever an unauthorized fingerprint is received. For example, the biometric lock **80** may emit a beeping sound and/or output a warning message. In an embodiment, the biometric lock **80** may be configured to automatically disable itself for a period of time if a user has attempted and failed to access the biometric lock a predetermined number of times.

[0030] In another embodiment according to the present disclosure, a suitcase may be provided. The suitcase may include a plurality of shells for forming storage compartments of the suitcase. The plurality of shells of the suitcase may comprise one or more hard-sided shells and/or soft-sided shells. The suitcase may also include a zipper mechanism for connecting the plurality of shells, wherein the zipper mechanism may be utilized to provide access to at least one storage compartment of the storage compartments. Furthermore, the suitcase may include a biometric lock configured to prevent unauthorized access to the at least one storage compartment of the storage compartments. The biometric lock may include a memory device configured to store a plurality of fingerprints. The biometric lock may further include a biometric reader, which may be configured to receive a fingerprint, wherein the biometric reader is configured to determine if the received fingerprint matches a stored fingerprint of the plurality of stored fingerprints. When the received fingerprint matches the stored fingerprint, the biometric reader may be configured to provide access to the zipper mechanism of the suitcase.

[0031] In yet another embodiment, another suitcase may be provided. The suitcase may include a plurality of shells utilized to form storage compartments of the suitcase. Additionally, the suitcase may include a fastening mechanism for connecting the plurality of shells. The fastening mechanism may be utilized to provide access to at least one storage compartment of the storage compartments of the suitcase. The suitcase may further include a biometric lock, which may be configured to prevent unauthorized to the at least one storage compartment of the storage compartments. The biometric lock may include a memory device configured to store a plurality of physical identifiers and the biometric lock may include a biometric reader. Notably, the biometric reader may be configured to receive a physical identifier and to unlock the biometric lock when the received physical identifier matches a stored physical identifier of the plurality of stored physical identifiers.

[0032] An exemplary method **400** of accessing a suitcase featuring a biometric lock may be provided as well. The method **400** may include storing authorized fingerprints and settings for the fingerprints **402**. The fingerprints and settings

for the fingerprints may be stored in a memory device of a biometric lock of the suitcase, such as biometric lock **80**. In an embodiment, the fingerprints and settings may be stored in a computing device which is connectable to the biometric lock and/or suitcase. The fingerprints may be classified as authorized or unauthorized fingerprints. Settings may include, but are not limited to including, a frequency at which a particular fingerprint can be utilized to access the biometric lock, an expiration date associated with a particular fingerprint, a time frame to access the biometric lock, a time period for automatically locking the biometric lock after access is provided to the biometric lock, rankings associated with the fingerprints, the ability to add or delete users/fingerprints, and administrator privileges.

[0033] Also, the method **400** may include receiving a fingerprint from a user for accessing the biometric lock of the suitcase **404**. The fingerprint from the user may be received by a biometric reader (e.g. fingerprint reader) of the biometric lock. The method **400** may include determining if the fingerprint from the user is an authorized fingerprint **406**. The determination may be performed by determining if the fingerprint matches an authorized fingerprint stored in the memory device or computer. If the fingerprint is an authorized fingerprint, the method **400** may include unlocking the biometric lock of the suitcase **408**. If, however, the fingerprint is either not stored in the memory device or computing device or is classified as an unauthorized fingerprint, the method **400** may include denying access to the biometric lock of the suitcase **410**. If the fingerprint is authorized to unlock the biometric lock, the method **400** may include granting permissions to the user based on the settings stored on the memory device and/or computing device **412**. Notably, the method **400** is not limited to the above method description and may incorporate any of the functionality and/or features described for any of the other embodiments disclosed herein.

[0034] The arrangements described herein are intended to provide a general understanding of the structure of various embodiments, and they are not intended to serve as a complete description of all the elements and features of apparatus and systems that might make use of the structures described herein. Many other arrangements will be apparent to those of skill in the art upon reviewing the above description. Other arrangements may be utilized and derived therefrom, such that structural and logical substitutions and changes may be made without departing from the scope of this disclosure. Figures are also merely representational and may not be drawn to scale. Certain proportions thereof may be exaggerated, while others may be minimized. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense.

[0035] Thus, although specific arrangements have been illustrated and described herein, it should be appreciated that any arrangement calculated to achieve the same purpose may be substituted for the specific arrangement shown. This disclosure is intended to cover any and all adaptations or variations of various embodiments and arrangements of the invention. Combinations of the above arrangements, and other arrangements not specifically described herein, will be apparent to those of skill in the art upon reviewing the above description. Therefore, it is intended that the disclosure not be limited to the particular arrangement(s) disclosed as the best mode contemplated for carrying out this invention, but that the invention will include all embodiments and arrangements falling within the scope of the appended claims.

What is claimed is:

1. A hard-sided suitcase, the hard-sided suitcase comprising:

at least two hard-sided shells, wherein the at least two hard-sided shells form storage compartments of the hard-sided suitcase;

a zipper mechanism, wherein the zipper mechanism is utilized to connect the at least two hard-sided shells and to provide access to the storage compartments of the hard-sided suitcase; and

a biometric lock attached to a portion of the at least two hard-sided shells, wherein the biometric lock is configured to lock the zipper mechanism and is utilized to prevent unauthorized access to at least one storage compartment of the storage compartments, wherein the biometric lock comprises:

a memory device configured to store at least one authorized fingerprint for accessing the suitcase; and

a fingerprint reader, wherein the fingerprint reader is configured to unlock the biometric lock when an authorized fingerprint of the at least one authorized fingerprint is received by the fingerprint reader, and wherein upon unlocking the biometric lock access is provided to the zipper mechanism so as to provide access to the at least one storage compartment of the suitcase.

2. The hard-sided suitcase of claim **1**, wherein the fingerprint reader is configured to receive a fingerprint from a user, wherein the fingerprint reader is further configured to determine if the fingerprint from the user is the authorized fingerprint of the at least one authorized fingerprint by determining that the fingerprint is stored in the memory device.

3. The hard-sided suitcase of claim **1**, wherein the fingerprint reader is configured to not unlock the biometric lock when the fingerprint reader receives at least one unauthorized fingerprint.

4. The hard-sided suitcase of claim **1**, wherein the at least one authorized fingerprint comprises at least one of an administrator fingerprint and a non-administrator fingerprint, wherein authorization and rights associated with the administrator fingerprint and the non-administrator fingerprint are set by an administrator associated with the administrator fingerprint.

5. The hard-sided suitcase of claim **1**, wherein the biometric lock is configured to lock at least one of a slider and a pull tab of the zipper mechanism, and wherein the fingerprint reader is configured to unlock at least one of the slider and the pull tab from the biometric lock when the authorized fingerprint of the at least one authorized fingerprints is received by the fingerprint reader.

6. The hard-sided suitcase of claim **1**, wherein the biometric lock is configured to be connectable to a computing device via a universal serial bus device, wherein the computing device is configured to store at least one of the at least one authorized fingerprint, a ranking associated with the at least one authorized fingerprint, and rights associated with the at least one authorized fingerprint.

7. The hard-sided suitcase of claim **1**, wherein the biometric lock comprises a power source for providing power to the biometric lock, wherein the power source comprises a battery comprising at least one of a lithium battery, an alkaline battery, a zinc-carbon battery, a nickel metal hydride battery, a nickel-zinc battery, and a nickel-cadmium battery.

8. The hard-sided suitcase of claim **1**, wherein the biometric lock further comprises a cover for concealing the fingerprint reader when not in use, wherein the cover is configured to adjust away from the fingerprint reader when a user adjusts the cover.

9. The hard-sided suitcase of claim **1**, wherein the hard-sided shells are comprised of at least one of polycarbonate, a polycarbonate composite, acrylonitrile butadiene styrene, polypropylene, plastic, wood, and metal.

10. A suitcase, the suitcase comprising:

a plurality of shells for forming storage compartments of the suitcase, wherein the plurality of shells comprise at least two hard-sided shells;

a zipper mechanism for connecting the plurality of shells, wherein the zipper mechanism is utilized to provide access to at least one storage compartment of the storage compartments; and

a biometric lock configured to prevent unauthorized access to the at least one storage compartment of the storage compartments, wherein the biometric lock comprises:

a memory device configured to store a plurality of fingerprints; and

a biometric reader, wherein the biometric reader is configured to receive a fingerprint, wherein the biometric reader is configured to determine if the received fingerprint matches a stored fingerprint of the plurality of stored fingerprints, and wherein the biometric reader is configured to provide access to the zipper mechanism when the received fingerprint matches the stored fingerprint.

11. The suitcase of claim **10**, wherein the plurality of stored fingerprints comprise administrator fingerprints and non-administrator fingerprints, wherein access rights associated with the administrator fingerprints and non-administrator fingerprints are set by an administrator.

12. The suitcase of claim **11**, wherein the access rights comprise at least one of a frequency at which the plurality of stored fingerprints can be utilized to access the biometric lock, an expiration associated with the plurality of stored fingerprints, a time period for automatically locking the biometric lock after access is provided to the zipper mechanism, and administrator privileges.

13. The suitcase of claim **10**, wherein the biometric lock is configured to lock at least one of a slider and a pull tab of the zipper mechanism, and wherein the biometric lock is configured to provide access to the zipper mechanism by unlocking at least one of the slider and the pull tab.

14. The suitcase of claim **10**, wherein the biometric reader is configured to deny access to the zipper mechanism when the received fingerprint does not match the stored fingerprint of the plurality of stored fingerprints.

15. The suitcase of claim **10**, wherein the memory device is configured to store the received fingerprint in an unauthorized fingerprint list when the received fingerprint does not match the stored fingerprint of the plurality of stored fingerprints, wherein the biometric lock is configured to emit a warning signal if the received fingerprint is received again.

16. The suitcase of claim **10**, wherein the biometric lock is configured to be connectable to a computing device via a universal serial bus device, wherein the computing device is configure to store the plurality of stored fingerprints and information associated with the plurality of stored fingerprints.

17. A suitcase, the suitcase comprising:

a plurality of hard-sided shells for forming storage compartments of the suitcase;

a fastening mechanism for connecting the plurality of hard-sided shells, wherein the fastening mechanism is utilized to provide access to at least one storage compartment of the storage compartments; and

a biometric lock configured to prevent unauthorized access to the at least one storage compartment of the storage compartments, wherein the biometric lock comprises:

a memory device configured to store a plurality of physical identifiers; and

a biometric reader, wherein the biometric reader is configured to receive a physical identifier, and wherein the biometric reader is configured to unlock the biometric lock when the received physical identifier matches a stored physical identifier of the plurality of stored physical identifiers.

18. The suitcase of claim **17**, wherein the fastening mechanism comprises at least one of a zipper mechanism, a snap fastener, a button, a buckle, and a tie.

19. The suitcase of claim **17**, wherein the biometric lock further comprises at least one of a power source for providing power to the biometric lock, a sliding cover for concealing the biometric lock, and a universal serial bus interface for connecting to a universal serial bus device.

20. The suitcase of claim **17**, wherein the biometric reader is configured to provide access to the fastening mechanism when the biometric lock is unlocked, and wherein the biometric reader is configured to not unlock the biometric lock when the received physical identifier does not match the stored physical identifier of the plurality of stored physical identifiers.

* * * * *