Technical Disclosure Commons

Defensive Publications Series

June 29, 2017

Verifying Authenticity of Currency and Tracking Duplicates

Mansoor Alicherry

Verifying Authenticity of Currency and Tracking Duplicates

To enable merchants and other persons to verify the validity and/or authenticity of paper currency notes, a digital signature can be applied to the currency notes. The digital signature is generated based on a serial number included on the note and a private key. Persons can verify the authenticity of the notes by sending either the serial number and signature, or a photograph of the note, to a server. The server can indicate whether the signature is valid for the serial number, indicating the authenticity of the note. In case of counterfeit notes that duplicate the serial numbers and signatures of valid notes, the server can track the verifications of notes, and if the same note is verified at remote locations within a short time span, the note, locations, and time can be flagged to follow up for a possible duplicated, counterfeit note.

Counterfeit currencies can cause harm to a cash-based economy. Counterfeit currencies can result in losses to innocent persons who unknowingly acquire the counterfeit currency notes, reduce confidence in the notes, and create national security issues by funding terrorist activities and human or drug trafficking. Central banks that issue currency notes can apply physical security features to the notes to prevent counterfeiting, such as security threads, watermarks, or raised printing. These features can require sophisticated technology or trained eyes to determine whether notes are fake. However, counterfeiters can still produce authentic-looking currency notes.

This publication proposes printing a digital signature on each note that can be verified by persons using mobile applications, such as smartphones with cameras, Internet connections, and appropriate software. The digital signature can be based on a serial number printed on the note and on a private key, and can appear on the note in the form of a Quick Response Code (QR code). The digital signature can add additional security to the currency beyond the physical security features. Persons can verify the authenticity of the notes with a central server by taking a photograph of the notes and sending either the photograph or the serial number and signature to the central server. Based on the verification requests, the server can report information regarding

fake or duplicated notes to appropriate authorities. The authorities can use the information to track down fake or duplicated notes.

FIG. 1 is a diagram showing a server 102 in communication with user equipments (UEs) 108A, 108B, 108C, 108D, 108E, 108F, 108G (collectively user equipments 108) via base stations 106A, 106B, 106C (collectively base stations 106) and a network 104. The network 104 can be any network via which computing devices communicate, such as the Internet. The base stations 106 can include any wireless devices that transmit or relay messages and/or data from the user equipments 108 to the server 102 via the network 104, and may be included in the network 104. The server 102 can include a computing device that responds to requests from the user equipments 108 to verify the authenticity of currency notes, and may receive and respond to the requests via the Hypertext Transport Protocol (HTTP). The user equipments 108 can include mobile devices such as smartphones and/or mobile devices that include cameras or other optical devices that capture images and are capable of sending and receiving messages to and from the server 102 via a wireless interface.

Users of the user equipments 108 can verify the authenticity of paper or other physical currency notes by taking pictures and/or photographs of the notes with the user equipments 108 and sending requests including either the pictures, or serial numbers and signatures recognized by the user equipment 108 based on the pictures, as well as location and time information, to the server 102 via the associated base station 106 and the network 104. The server 102 can respond to the requests by sending a message indicating that the note is authentic or not authentic. In the case where the note is not authentic, the server 102 can send an instruction to the user equipment 108 indicating steps for the user to take, such as taking the currency note to a bank for further verification. In the case where the note is not authentic, the server 102 can also report the

inauthentic note to the authorities, who may investigate counterfeit activity near the location included in the request. The response by the server 102 to the user equipment 108 enables anyone with a smartphone and the appropriate application installed on the smartphone to verify the authenticity of a currency note offered to them in a cash transaction. In the case where the note is authentic, but a note with an identical serial number and identical signature was authenticated at a location remote from the request close in time to the request, the server 102 can report a possible duplicated note to the authorities, who may investigate possible counterfeit activity near the locations included in the requests. In addition to tracking down crime, the monitoring of cash transactions by verifying authenticity of currency notes enables a central entity, such as the government that issued the currency notes, to track macroeconomic activities associated with the flow of currency notes.

FIG. 2 is a block diagram showing a workflow for creating digitally signed currency notes. A currency generation server 202 can determine serial numbers for currency notes, and signatures for the currency notes based on the determined serial numbers, a private key ($P_{Private}$), and optionally a secret phrase (K). The secret phrase K can be different for different denominations of currency, and/or different key pairs can be used for different denominations of currency. Similarly, the private key $P_{Private}$ and/or secret phrase K can be different for different series of the currency. The private key $P_{Private}$ can be part of a key pair ($P_{Private}$, P_{Public}) that the currency generation server 202 generated using a public key cryptography system such as RSA or DSA. The length of the keys $P_{Private}$, P_{Public} should be long enough to withstand any brute force attack during the life of the currency, such as at least 4,096 bits long for RSA, or an equivalent strength in DSA. The private key $P_{Private}$ can be a private key that is securely maintained by the server 202. To protect the private key $P_{Private}$, the server 202 can be maintained

on an isolated network that is not accessible from any public network such as the Internet. The public key P_{Public}, which can be used to authenticate a signature by verifying that a holder of the private key $P_{Private}$ generated the signature, can be maintained by servers such as the server 102 that is accessible by mobile applications running on the user equipments via a public network such as the Internet. Maintaining the public key P_{Public} on the server 102, rather than distributing the public key P_{Public} to the user equipments, can eliminate the need to update applications when the public key P_{Public} changes, and can require users to send requests to the server 102, enabling the server 102 to collect data about currency flow and possible counterfeit currency. In countries and/or geographic regions with poor network connectivity, the public key P_{Public} can be stored on the user equipment 108 for the user equipment 108 to verify the signature, with the user equipment 108 reporting, to the server 102, information required to detect duplicates and/or counterfeit notes when a connection between the user equipment 108 and server 102 through the network 104 becomes available.

The currency generation server 202 can generate unique serial numbers for each note by assigning serial numbers sequentially. The currency generation server 202 can, optionally, append the secret phrase (K) to the serial number to generate a message (M). The message M can optionally include information on the currency note, such as the denomination and/or value of the currency note. The currency generation server 202 can compute a secret hash value (H) on the message and the secret phrase (M, K). The currency generation server 202 can compute the secret hash value H using a cryptographic safe hash function such as SHA256. After determining the hash value H, the currency generation server 202 can generate a signature (S) based on the secret hash value H and the private key $P_{Private}$. The currency generation server 202 can generate the signature S based on the secret hash value H and the private key $P_{Private}$ using the RSA

signature algorithm or the Digital Signature Algorithm (DSA). The currency generation server 202 can send the generated serial number and signature *S* (206) to a currency print server 204.

The currency print server 204 can print, and/or instruct a printer to print, currency notes based on the generated serial numbers and signatures *S* (206) that the currency print server 204 receives from the currency generation server 202. The currency notes printed by the currency print server 204 and/or upon instruction by the currency print server 204 can include the serial numbers and signatures *S* (206) received from the currency generation server 202, as well as denominations of the notes and artwork or other insignia such as portraits of famous persons. The currency print server 204 can send print status messages 208 to the currency generation server 202. The print status messages 208 can indicate which serial numbers have been applied to currency notes.

FIG. 3 is an example of a note 300 printed by the currency print server 204 as described above. The note 300 can include the serial number 302 received by the currency print server 204 from the currency generation server 202. The serial number 302 can be unique for each note 300, so that no two authentic notes have the same serial number 302. The note 300 can include artwork or other insignia, such as a portrait 304 of a famous person in the country that printed the note 300, and/or physical security features such as watermarks, security thread(s), and/or raised printing.

The note 300 can include the digital signature 306. The digital signature 306 can be printed in the form of a Quick Response Code (QR code) or other format easily recognized and/or interpreted by a computing system such as any of the user devices 108 and/or server 102. The note 300 can also include a denomination 308 indicating the value of the note 300.

FIG. 4 shows a user equipment 108 taking a picture of a note 300. The user equipment 108 includes a camera 402 that captures optical information such as printed matter on the note 300. A user, who may be selling a good or service in exchange for the note 300, can take a picture of the note 300 using the camera 402 included in the user equipment 108. The camera 402 can capture at least the serial number 302 and the signature 306 included on the note 300, and optionally other information such as the denomination of the note 300 and the condition of the note 300.

An application installed and/or running on the user equipment 108 can perform optical character recognition on the captured image to extract the serial number and signature (206) from the captured image and send the serial number and signature (206) to the server 102 for verification, or send the captured image to the server 102 and let the server 102 perform the optical character recognition on the captured image. The application running on the user equipment 108 can receive a message from the server 102 indicating whether the note 300 is authentic, and the user equipment 108 can present a message or other indicator to the user indicating whether the note 300 is authentic.

FIG. 5 is a block diagram showing a currency verification and fake currency detection system. As described above, the user equipment 108 captures an image 502 of the note 300. The user equipment 108 sends note data 502, which may include the serial number and signature extracted by the user device 108 from the image 502, or the image 502 itself, to the server 102.

The server 102 can determine the authenticity of the note 300 based on the serial number and signature. If the note data 504 included the image 502 rather than the extracted serial number and signature, then the server 102 can perform optical character recognition to extract the serial number and signature from the image 502. Batch application program interfaces (APIs)

implemented by the server can receive requests for multiple notes 300 and can return the verification results for the multiple currencies in a single response.

The server 102 can verify the authenticity of the note 300 by performing a hash function on the serial number *M* of the note 300 and the secret phrase *K* to compute a hash value *H*. The server 102 can authenticate the note by verifying the signature *S* for the hash *H* using a "public" key (P_{Public}), which is known only to the server 102 and/or administrators of the server 102. The server 102 can send a validity indicator 506 to the user equipment 108 indicating whether the note 300 is authentic based on whether the signature is a valid signature for the serial number. To encourage users to make frequent requests about whether notes are authentic, the server 102 could send interesting information about the notes such as the locations that the notes have traveled through. The server 102 can save the request including the note data 504 for future analysis, such as by an analyzer 508.

Counterfeiters can create fake currency either by creating fake notes with serial numbers and signatures created by the counterfeiters, which are unlikely to be verified by the server 102, or by duplicating the serial numbers and signatures of authentic notes. The server 102 can send log information 512 to an analyzer 508. The log information 512 can include the serial numbers, signatures, and denominations of notes verified by the server 102, as well as times and locations of the user equipments 108 at the times the requests for verification were made.

The analyzer 508 can determine when requests for verification of notes with the same serial number were made so close in time but far away in location that the two transactions likely did not involve the same physical note, or when the frequency of verification requests for a particular serial number is higher than would be expected if a single note carried that serial number, or when the location of a note with a particular serial number changes faster than would

be expected if a single note carried that serial number, and likely involved a duplicate of a note created by a counterfeiter. The analyzer 508 can, for example, run periodic analysis on the log information 512 generated by the server 102, and identify currency notes that are likely to have duplicates. The analyzer 508 can group the likely duplicate notes by location to identify the locality(ies) that have been affected by the counterfeit currency. The authorities can trace the path that the notes took to find the location of the source of the counterfeit currency.

The analyzer 508 can send duplicate reports 516 to a currency monitor 510, indicating the times and locations of requests to verify notes with the same serial number. The server 102 can also send mismatch reports 514 to the currency monitor 510 when the server 102 determines that a signature does not match the serial number of a note for which a request for verification was received. The mismatch reports 514 can include the serial number, signature, and denomination of the currency, as well as the time and location of the user equipment 108 that made the request for verification of the authenticity of the note.

The currency monitor 510 can monitor the mismatches 514 and duplicates 516. The currency monitor 510 can alert the authorities, such as police, of mismatches 514 and/or duplicates 516, who can then track down the counterfeit notes close to their source. The currency monitor 510 can also alert users having counterfeit, duplicated currency notes. The users can be requested to bring the currency notes to a bank to distinguish duplicated, counterfeit notes from original, authentic notes.

The currency monitor 510 can also track macroeconomic activities and identify potential black money. The currency monitor 510 can track commerce by analyzing trends in economic activities based on verification requests, which can indicate flows of currency to different geographic areas and trade between the different geographic areas. The currency monitor 510

can track currency flows based on counterfeit detection machines at banks and large businesses making verification requests, reducing transactions in illegal goods and services. The currency monitor 510 can also track currency notes that are stored rather than spent based on the notes not being verified, which may indicate a person engaging in illegal activity maintaining a large store of cash. The currency monitor 510 can also track potential problem areas based on inferences that areas in which verification requests are made more frequently have lower levels of trust in economic transactions.

FIG. 6A is a diagram showing a single currency note 300 being duplicated with multiple copies 300A, 300B, 300C, 300D. A counterfeiter can make multiple copies 300A, 300B, 300C, 300D of a single note 300, using the same serial number and signature so that the server 102 will verify the copies 300A, 300B, 300C, 300D as authentic, to create a large amount of counterfeit currency. However, the presence of multiple copies 300A, 300B, 300C, 300D with the same serial number and signature increases the likelihood that the analyzer 508 will detect the presence of duplicates 516, enabling the authorities to track the copies 300A, 300B, 300C, 300D back to their source.

FIG. 6B is a diagram showing multiple currency notes 300A, 300B, 300C, 300D each being duplicated with a single copy 300A, 300B, 300C, 300D. In this scenario, the counterfeiter can create a single counterfeit note and/or copy 300A, 300B, 300C, 300D from each authentic note 300A, 300B, 300C, 300D. Creating only a single counterfeit note and/or copy 300A, 300B, 300C, 300D from each authentic note 300A, 300B, 300C, 300D reduces the number of duplicates 516, making the counterfeiter harder to detect by the currency monitor 510 based on duplicates 516 reported by the analyzer 508. However, creating only a single counterfeit note and/or copy 300A, 300B, 300C, 300D from each authentic note 300A, 300B, 300C, 300D also

requires the counterfeiter to start with a larger amount of currency, and reduces the amount of counterfeit currency that he or she can create based on the authentic currency that he or she has.

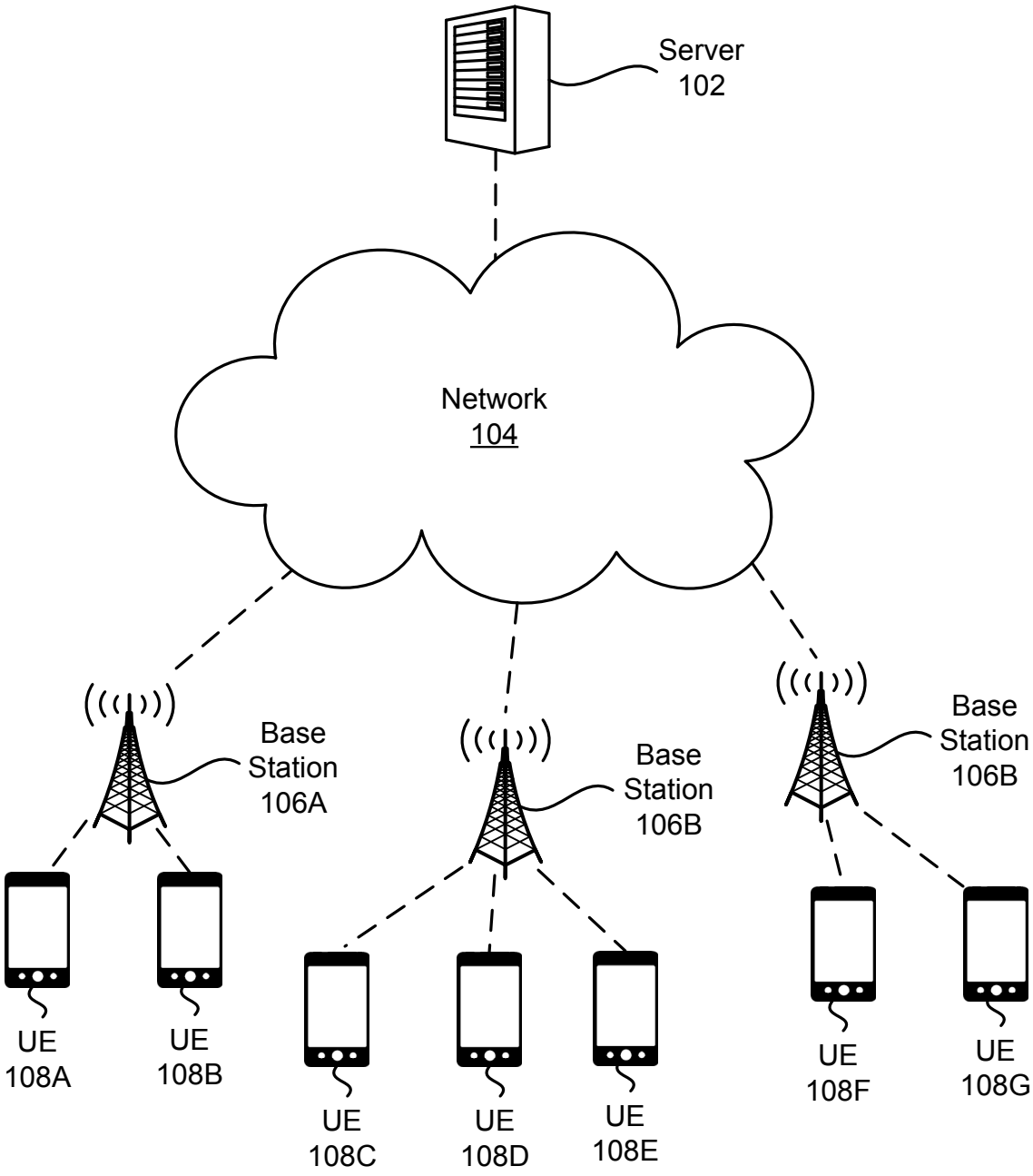
Server
102
Network
104
Base
Station
106A
Base
Station
106B
Base
Station
106B
UE
108A
UE
108B
UE
108C
UE
108D
UE
108E
UE
108F
UE
108G

FIG. 1

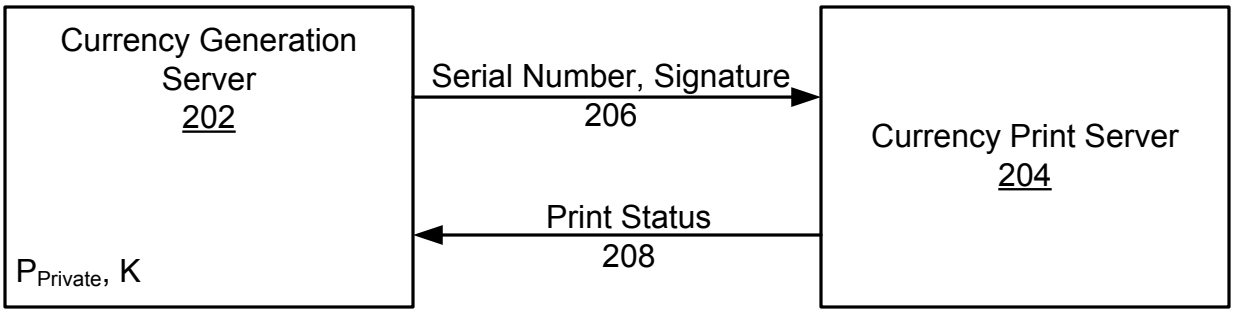
Currency Generation Server
202
$P_{Private}$, K
Serial Number, Signature
206
Print Status
208
Currency Print Server
204

FIG. 2

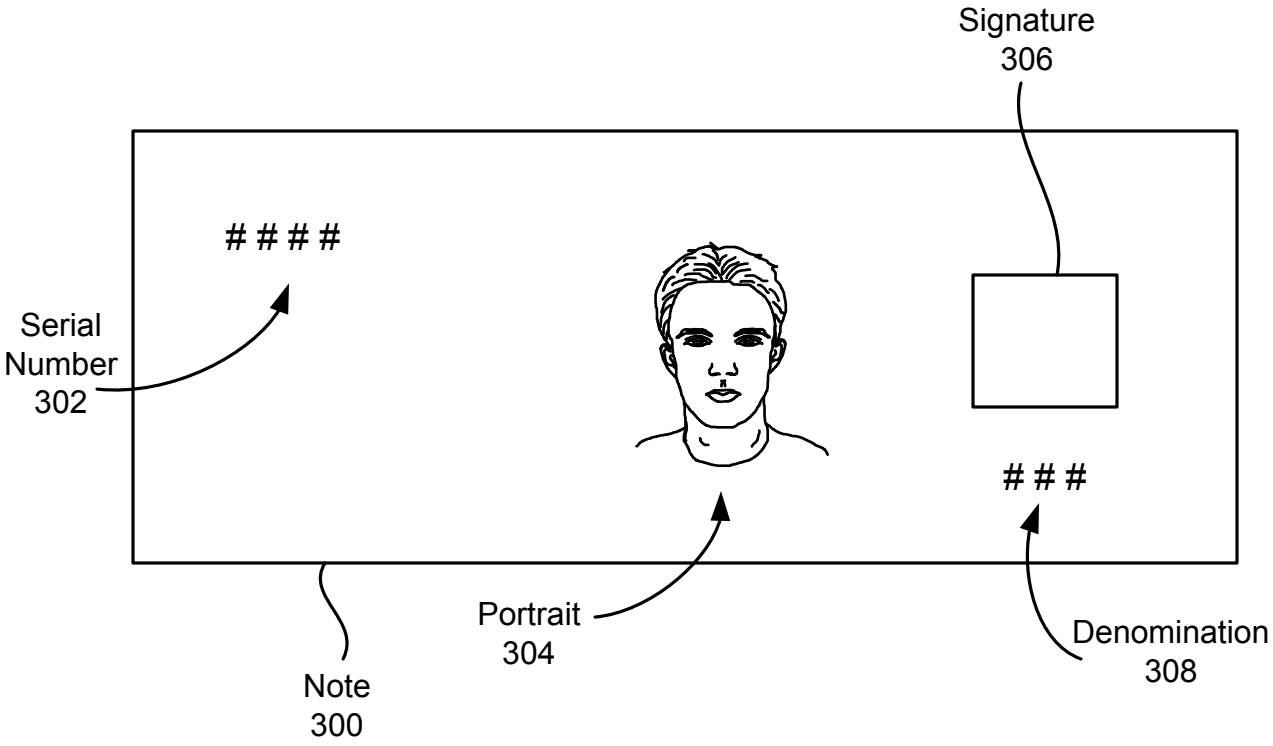
Signature
306
####
Serial Number
302
###
Portrait
304
Denomination
308
Note
300

FIG. 3

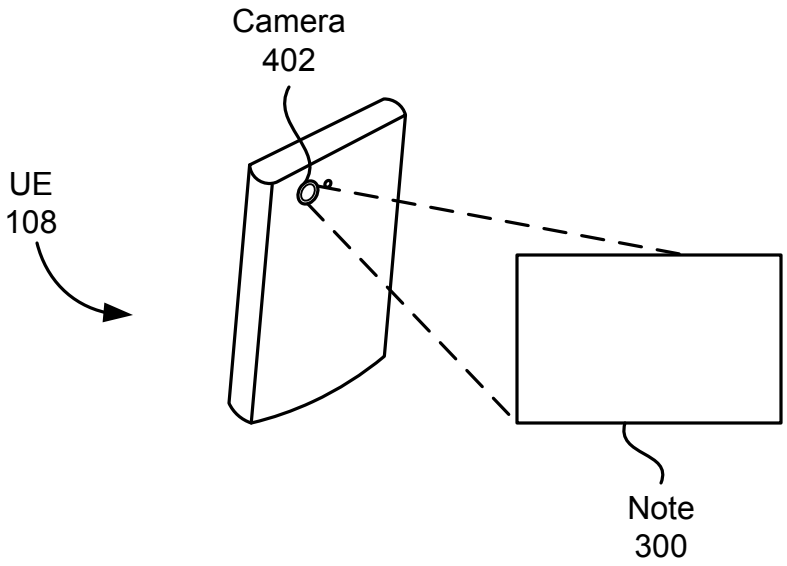
Camera
402
UE
108
Note
300

FIG. 4

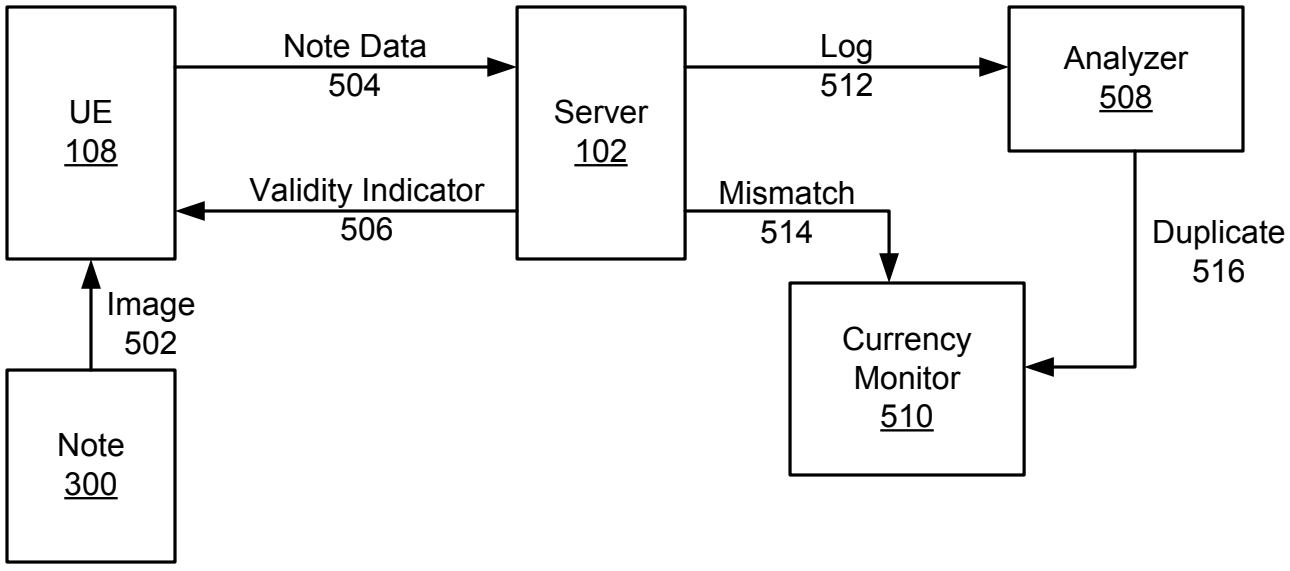
UE
108
Note Data
504
Server
102
Log
512
Analyzer
508
Validity Indicator
506
Mismatch
514
Duplicate
516
Image
502
Currency
Monitor
510
Note
300

FIG. 5

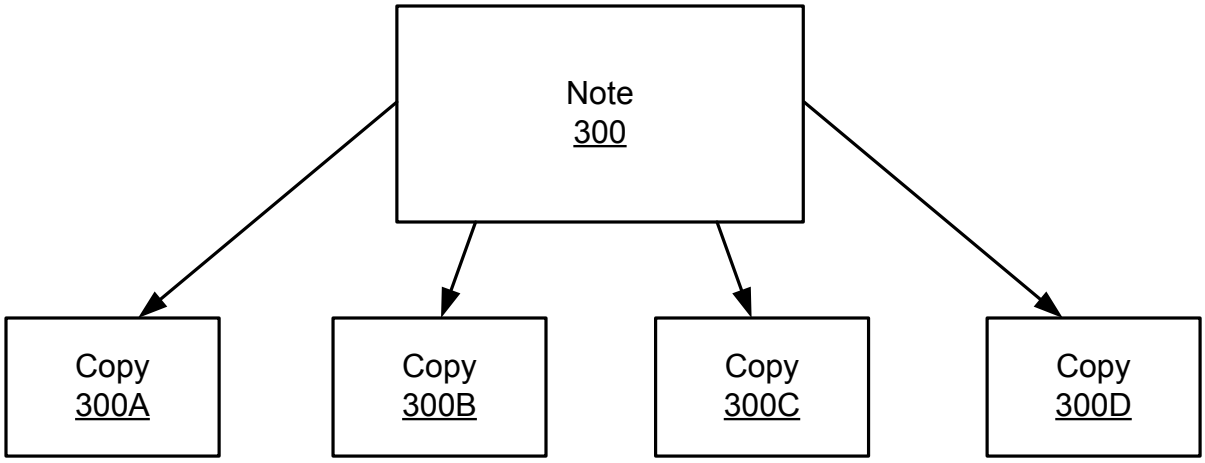
Note
300
Copy
300A
Copy
300B
Copy
300C
Copy
300D

FIG. 6A

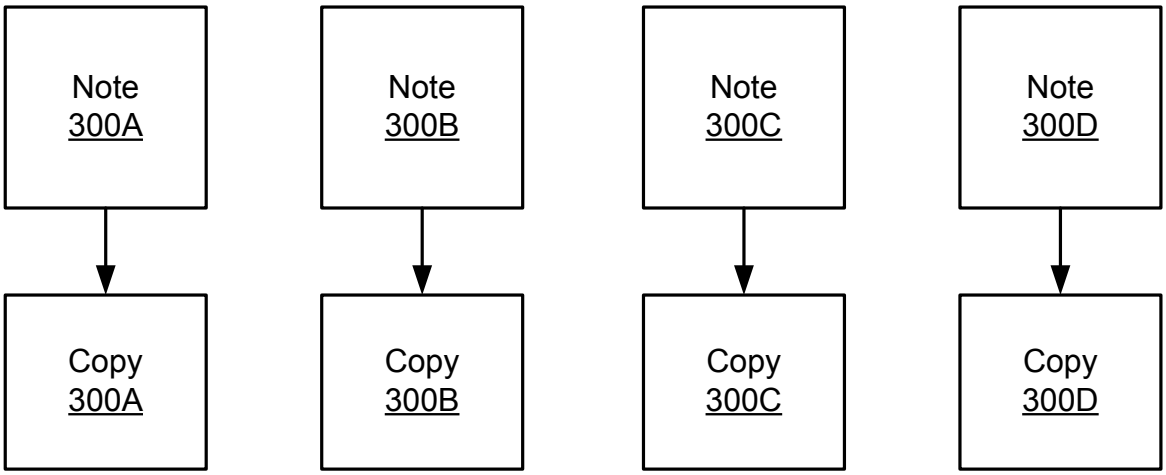
Note
300A
Note
300B
Note
300C
Note
300D
Copy
300A
Copy
300B
Copy
300C
Copy
300D

FIG. 6B