'J'] 1 E TRUSTWORTHY DIGITAL CAMERA : RESTORING CREDIBILITY TO THE PHOTOGRAPHIC IMAGE

Gary 1.. Friedman
Technical Group I .eader
Advanced Engineering ant] Prototype Group
Jet Propulsion 1 ,aboratory
California institute of Technology
Pasadena, CA 91109

introduction

The increasing sophistication of computers has made digital manipulation of photographic images (as well as other digital ly-recorded artifacts, such as sound and video) incredibly easy to perform and, as time goes on, increasingly difficult to detect. Today, every picture appearing in newspapers and magazines has been digitally altered to some degree, with the severity varying from the trivial (cleaning up "noise" and removing distracting backgrounds) to the point of deception (articles of clothing removed, heads attached to other people's bodies, the complete rearrangement of city skylines). As the power, flexibility and ubiquity of image-a]lcriJlg computers continues to increase, the well-kJIown adage that "the photograph doesn't lie" will continue to become an anachronism.

A solution to this problem comes from the proposed Digital Signature Standard (11SS), which incorporates modern Cryptographic techniques to authenticate el ectronic mail messages. [1] [2] ("Authenticate" in this case means you can be sure that the message has not been altered, and that the sender's identity has not been forged.)

Background on Digital Signatures

The Digital Signature Standard (DSS) builds upon a recent encryption technique called "Public Key Encryption" [3]. Older encryption/decryption schemes require that both the sender and receiver possess the same secret "key": the sender uses the key to transform the text message into ciphertext, and the receiver uses the same key to perform an inverse transformation on the ciphertext, revealing the original text message. If the correct key transforms the ciphertext into unreadable garbage, it is reasonable to conclude that either the wrong key is being used, the message has been altered, or the sender has been impersonated by someone ignorant of the correct key. The historic drawback to this secret key encryption scheme has been in the secure distribution of keys; key disclosure must occur out-of-band, either transmitted via an expensive alternate path or arranged when sender and receiver were proximate.

Public key encryption techniques differ in that they enable the recipient of a message to decrypt it using a key that is different from the one. used by the sender to encrypt it, All public key cryptography is based on the principle that it is easy to multiply two large prime numbers together, but extremely difficult (taking perhaps centuries using today's supercomputers) to work backwards and uncover the factors that could have been used to generat c the result i ng number.

Public Key Encryption employs two different keys: a private key, which is held by the more security conscious party, and a public key, which is unique to the private key and can bc common knowlcdgc. Thc private kcy is sclcctcd by thc User; thcn thc public kcy corrcsponding to this privatc kcy is gcncratcd mechanically by the. encryption tcchnology.

'1'0 scnd a sccrct message that only thc rccipicnt can read, thc rccipicnt would first make his/hcr public kcy known to thc scndcr via any non-sccurc mcdium, such as a lcttcr, a tclcphonc conversation, or a ncwspapcr ad. Anyone wishing to scnd a sccurc message would encrypt thc mcssagc using this public kcy and scnd it to thc rccipicnt. Thc rccipicnt, having SOIC possession of the corrcsponding private. key, is the only onc able to dccrypt the message, Thc need to transmit a sccrct kcy that both parties must possess bcforchand has been climinatcd. Thc tradcoff in this case is that, although only the rccipicnt can read thc message, anyone who obtains the public kcy can scnd a message with anonymity. [1]

Thc process dcscribcd above can also bc implcmcntcd “backwards” to great advantage. in this second scenario, it is thc scndcr who maintains possession of the private key, and anyone who has thc widely disscminatcd corresponding public kcy decrypt any message cncryptcd with that private key. Although this proccdurc no longer pcrforms the traditional function of encryption (which is to provide confidential communication bctwccn two parties), it dots provide a way to insure that messages arc not forged: only the private kcy could have produced a message that is dccipherablc by the corresponding public kcy,

This gives us the foundation for message authentication: if the private kcy remains private, thcn *only* thc private kcy bolder can producc messages dccipherablc by tbc public key. Furthermore, it is cxtrcmcly difficult to rcvcrsc-cnginccr tbc public kcy and ascertain the original private key, Without knowlcdgc of thc private key, a counterfeit message cannot bc forged.

Digital signatures build upon these public kcy cryptographic techniques and allow you to authenticate thc contents of tbc message as wc]] as thc identity of the scndcr. Thc signatures arc produced by creating a *hash*[2] of thc plaintcxt message, and then encrypting the hash using thc scndcr's private key. Thc result is a second digital file (rcfcrrcd to as a *signature*) which accompanies the original plaintcxt message. “1”0 cmphasizc: THE ORIGINAL MESSAGE IS UNTOUCHED; only the message's hash is cncryptcd. This way the origins] filc can bc read by all, yet if yOLI wish to authenticate it you can decrypt thc message's uniquc digital signature using thc public key. If the dccryptcd digital signature and an indcpcndcnt hash on thc file in question match, both the integrity of thc message and thc authenticity of the sender can bc assured.

[1] Thc dcscribcd scenariocan also bc used as thc first stcp in a process of cxchanging sccrct keys to allow for conventional sccurc message transmission, climinating any of thc drawbacks of thc onc-way authcnticatability. [1], [4]

[2] A hash is the product of a bashing function; it is a mathematical function which maps values from a large domain into a smaller range. For example, dividing a binary filc into a collection of, say, 16 Kilobit pieces and performing a cumulative Exclusive OR function bctwccn successive pieces produces a simple 16 Kilobit “hash” which is smaller than the original file yet is practically unique to it. (Many more complex and secure. transformations are also possible.) Changing a single bit in the original message produces a very diffc.rent hash output; and reverse engineering a message so it will have a given hash value and also make sense to the reader is virtually impossible. A digital signature can then be created by encrypting the hashing output using the. sender's private key.

I low It Works

This digital signature technique is very general; it can bc applied not only to 1-dimensional symbolic text (such as electronic mail) but also to any n-dimensional digital pattern (such as digital video, digital audio, and/or digital holograms).

Standard digital cameras arc filmless; they sense light and color via an electronic Charge Coupled Device (CCD), and produce as output a compute.r file which describes the image using 1‘s and O’s arranged in a meaningful, prc-defined format. Often this digital image file is stored cm a small mass-storage medium inside the camera itself (such as floppy disk or magneto-op(ical disk) for later transference to a large computer. Alternatively, the image file can bc sent directly to the. computer via a transmission medium. once inside the computer it then can bc read and then easily altered in any number of different ways.

in the proposed digital camera wc wish to authenticate the initial image file as it emerges from the camera. (See Steps 1 -4.) To accomplish this, the camera produces two output files for each captured image: the first is an all-digital industry-standard file format representing the captured image. The second would bc an encrypted “digital signature" produced by applying the camera's unique private key (embedded within the camera’s microprocessor) to a hash of the capt ured image file, using the procedure described in [4]. It is the responsibility of the user to keep track of both files once they leave the Camera, since both arc required to authenticate the image.

Once the digital image file and the digital signature arc generated by the camera and Stored in computer memory, the image file's integrity can later bc affirmed by using a public key decoding program, which can bc freely distributed to users and Certification authorities via conventional software distribution techniques. This verification program, which has no knowledge of either the public or private, keys, takes as input the digital image file in c] uestion, its accompanying digits] signature file, and the public kcy which is unique to the originating camera. (It is perfectly reasonable to have the public kcy double as the camera’s serial number.) The program then calculates its own hash on the digital image file (the hashing algorithm need not bc kept a secret), and uses the public key to decode the digital signature to reveal the hash originally calculated by the camera at the time the image was taken.]f these two hashes match, it is certain to any required degree that the digital image in question is indeed identical to what the camera Originally produced. If on the other hand at least a single bit is different, the two hashes will not even closely match and the image’s integrity will not bc affirmed.

]f the technique is to bc effective (i .c., no false positives or false negatives) and extended to larger data sets such as digital audio, digital video or digital holograms, wc must build upon the accomplishments of the computer mass storage industry, which has already achieved the ability to store and deliver extremely large binary data sets without errors. Analog techniques (such as audio cassette tape or the NTSC encoding on today’s video tape formals) or non-corrected digital formats (such as the popular Philips' audio CD, which is so unreliable that CD player manufacturers now utilize "oversampling" to combat the problem of missed bits) introduce a large amount of errors upon playback which arc normally imperceptible to the human viewer/listener, but arc into] crable for the purposes of image authentication.

Mcasurcs of l'rotcction

1'hc schcmc as dcscribcd abovc is rcsistant to forgcry attcmpts sincc the sccrct privatc kcy (which is known only by thc camera's manufacturcr) is cmbcddcd in a probc-proof microproccssor which itsclf is dccply intcgratcd into the camera's systcm. (I'igurc 1.) I:vcn if some adcpt pirate were to dissect the camcra and rcplacc the chip with onc containing a homcbrcw key, the digital signature produccd thcrcaftcr would not bc dccodablc by any public kcy pub] i shcd by thc manufacturer.

1'hc advantagcs to freely distributing thc verification softwarc and valid public keys arc great; with thc softwarc freely available verification can bccomc commonplace and routinc. No special ccrtification authority nccd bc callcd in for routine chccks, no fees arc required, no big fuss is made, and no bad-faith climate amongst the parties involvcd need bc crcatcd as a rcsult of bcing challcngcd. But thc mass distribution of verification software docs carry onc danger: it would bc easy for somconc to crcatc a bogus program which looks, behaves, and has thc same file length as the genuine verification softwarc, with the only diffcrcncc being it always proclaims a "match" regardless of thc integrity of thc imagc being vcrificd. With thc software freely and widel y available this is not a large risk, as additional copies can bc easily obtaincd from multiplc sources and a best 2-out-of-3 schcmc can bc cmploycd. Whcn the slakes arc high and it is cxtrcmcly important that the verification software bc known to bc genuine, an indcpcndcnt certification authority or the manufacturcr could then bc callcd in to providc their own topic.s of the software and their own lists of public keys at the time of verification.

1'hc algorithms and private kcy ncccssary for encrypting the additional digital signature file from within the camera arc to bc cmbcddcd inside a ncw breed of sccurc microprocessors whosc ROM contents cannot bc obscrvcd outsidc of the factory, such as the Philips 83C852 microcontrollcr [5]. Bccausc the private kcy uscd for encryption is hard-codcd into this chip by thc manufacturer (who must then ensure the private key remains a sccrct), credibility of thc camera's output bccomcs an extension of that of the manufacturer; a digital signature from the camera can bc considcrcd to bc just as reliable and sccurc as if thc signature had been gcncratcd by thc manufacturcr.[3]

I:ach camcra should possess its own unique pair of private and public keys, with the private kcy ctchcd into the camera's sccurc microcontroller and the public kcy stored in three placcs: in a public kcy list kept by the manufacturcr, on the camera body itself (which can then also doublc as the camera's serial number), and in thc colorful specifications border (scc "Variations on a 1'hcmc" section bclow for a description of the border.) Assigning uniquc keys to each camera has thc benefit of avoiding instant obsolcsccncc which would occur if only onc private kcy were uscd for all camcras, and that kcy were to bc compromised, An even highcr lcvcl of security would occur if the manufact urcr were to destroy all records of the private kcy once thc camcra is produccd. (At that point thc private kcy is no longer nccdcd.) 1'his would eliminate the possibility of compromise via industrial cspionagc or theft,

I'inally, rcgular and free distribution of al] valid public keys is dcsirablc to defeat a countcrfcitcr who has lcarncd of the encryption algorithm cmploycd and has written a program to produce digital signaturcs based on his own private key. Dccoding these

[3] Any company involved with thc dcvclopmcnt of a 1'rustworthy Digital Came.ra would havc to address thc issuc of liability, for if thc security of the private. kcy wcrc cvcr to be compromised (for example by a disgruntlcd cmploycc who steals a private kcy ancl uses it to gcncratc false authcnticatablc images), the lawsuits brought on as thc rcsult of a false positive. would ncccssitatc significant insurance covcragc.

forgeries would require the use of a public key not generated by the manufacturer. Freely distributing updated public key lists would make it easy to identify and thwart such attempts.

Uses

The single most obvious use of a trustworthy camera would be in situations where proof of image authenticity is necessary; such as in courtroom proceedings or insurance claims. Today it is becoming common practice for insurance claims phonography to be done digitally; the. images are easily downloaded into a computer and ail the relevant information can be stored on-line in one place. Employing a trustworthy digital camera for this function could mean a seamless transition for evidence collectors, since the trustworthy camera is operated the same way as its conventional digital camera counterpart. (Ironically, simultaneous advancements in computer crimes and image manipulating tools will make it very easy in the future to commit insurance fraud by breaking into systems and convincingly altering the digital images. Company-wide employment of the proposed trustworthy camera will eliminate this risk.)

This technique need not be limited to still digital images. Because digital signatures can be used to verify any block of digital data, it can aiso be engineered into digital video cameras and digital audio tape recorders. in both these devices, a digital signature can be generated anti recorded onto **the** medium each time the recording process stops or pauses; this way each sound byte or video "take" is hashed, encoded and written at the time it's created,

Variations on a Theme

Since the proposed camera is being initially targeted towards courtroom authentication, a few additional features can be implemented to better serve this field. A bright]y-colored border could automatically be generated as part of each captured image file, Within the border would appear textual information about the image: the date and time it was taken, the ambient light level seen by the camera at the time of exposure, the original color temperature of the scene, the software version of the camera's firmware, the camera's serial number, the focusing distance of the lens at the time of exposure, a unique sequence number, and (when the technology allows for a Global Positioning System (GPS) receiver to be build into the camera) the geographical coordinates of the camera, indicating where in the world you were when the picture was taken. The ambient light level and color temperature readings would be useful for getting a fee] for exactly what the scene was like at the time of exposure; something a sensitive optical element might inadvertently hide via automatic exposure and color correction. The lens' focused distance is there to help detect potential abuse of the trustworthy camera: taking close-up pictures of a modified photo and trying to pass it off as an unaltered original. Since all these textual data in the colored border are part of the authenticated image file, their credibility are also upheld when authenticated by the public-key verification software.

The accuracy of the date and time information would again be the responsibility of the secure microprocessor; in addition to being able to keep its programming a secret, it also would have a lithium battery powering a system clock that was set to Universal (Greenwich Mean) Time at the time of manufacture. If the timer circuit ever fails or is tampered with the. system will be programmed to fill the time anti date fields with X XXX'S, eliminating the chance of a random time stamp being mistaken for the actual time.

Higher Level of Security

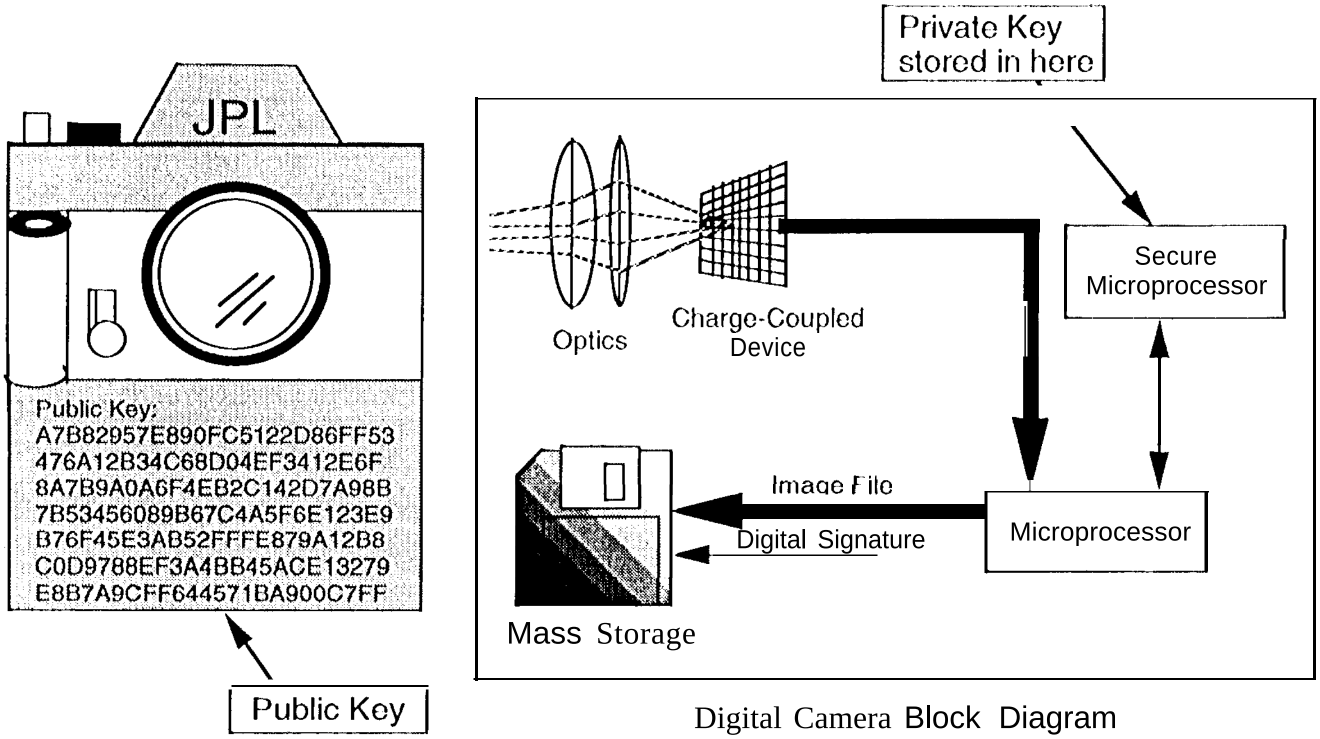
Although the proposed Trustworthy Digital Camera generally offers a satisfactory level of security, nevertheless there still exists a small possibility that a determined saboteur will be able to crack the camera's private key given an extended amount of time, (No cryptographic scheme will protect your data forever; given sufficient time, advancements in code breaking or improved computer horsepower will be enough to render any given level of cryptographic protection obsolete.) If the discovered private key were then to be published, it would allow an individual to generate authentic-looking digital signatures on altered image files, essentially undermining the credibility offered by the compromised camera. (The security level of other cameras in use, and of images taken with those cameras, will still remain high.)

Still, it would be wise to regularly Llp.grade and enhance the sophistication of the encryption implementation as newer camera models are introduced, typically using longer encryption/decryption key lengths, then later using improved encryption/ decryption algorithms, It is expected that evolving verification software (the public domain software component of this authentication scheme which is freely distributed) will then be designed to recognize, identify and authenticate all previous versions. Because the encryption details must necessarily be c.hanged often (depending on the technological capabilities of the day), no single key length or digital signature algorithm is being specified in this disclosure (although the National Institute of Standards and Technology's (NIST) Digital Signature Standard (DSS) was in mind when this proposal was conceived).

Conclusion

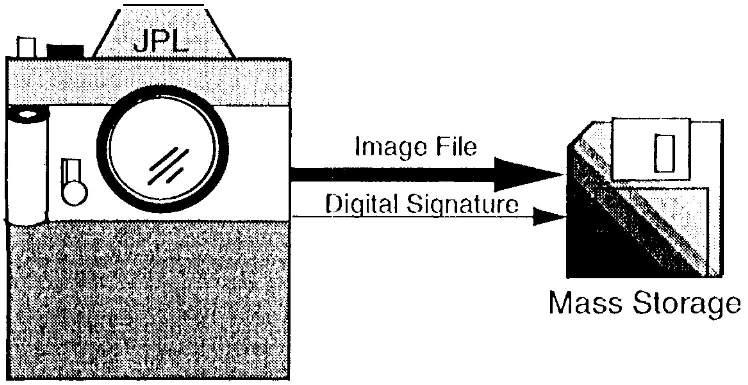
The Trustworthy Digital Camera is an application of existing technology toward the sol ution of an ever-nlorc-troLlbling social problem, the reliability of testimony. Although it will always be possible to lie with a photograph (using such titnc-honored techniques as false perspective and misleading captions), this proposed device will prevent the explosion of very capable persona] computers from driving up the incidence of doctored photographs being passed off as truth.

The research described in this paper was carried out by the Jet l'repulsion 1 Amatory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

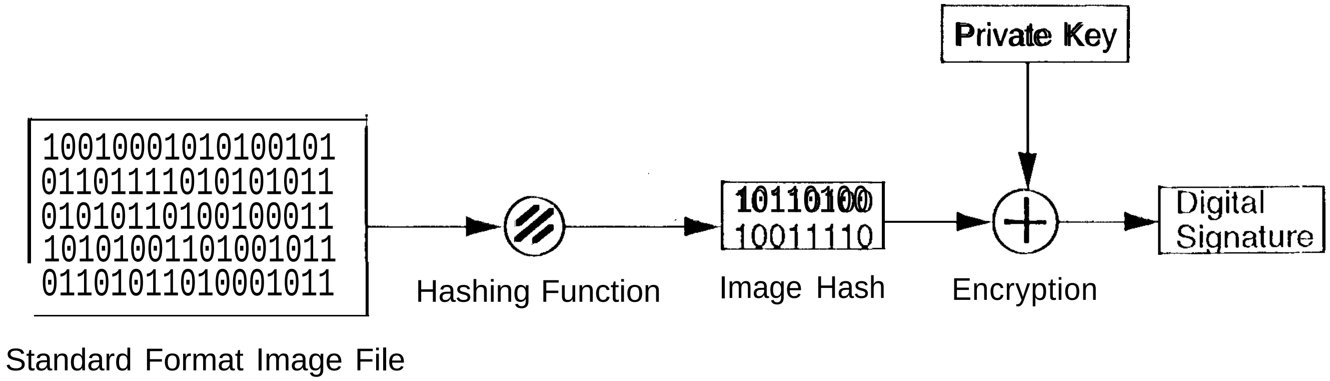


Digital Camera Block Diagram

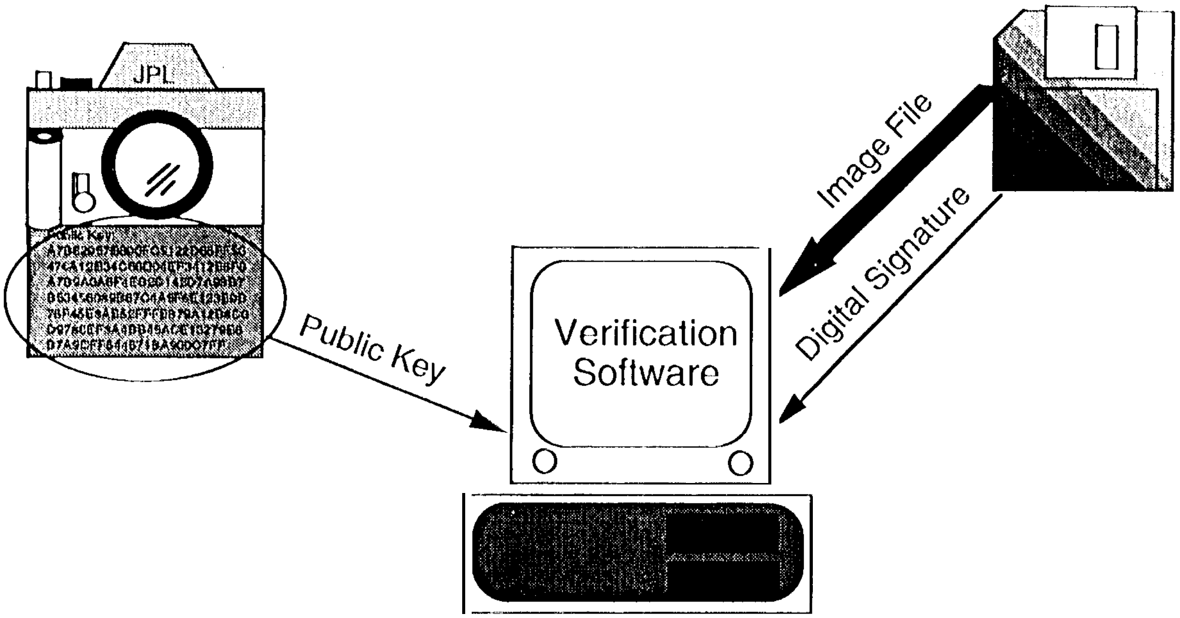
Figure 1: The Trustworthy Digital Camera starts with a digital sensor instead of film, and delivers the image directly in a computer-compatibile format. The secure microprocessor responsible for the encryption of the digital signature is programmed with the private key at the factory. The public key necessary for later authentication appears in the image's border as well as on the camera body.



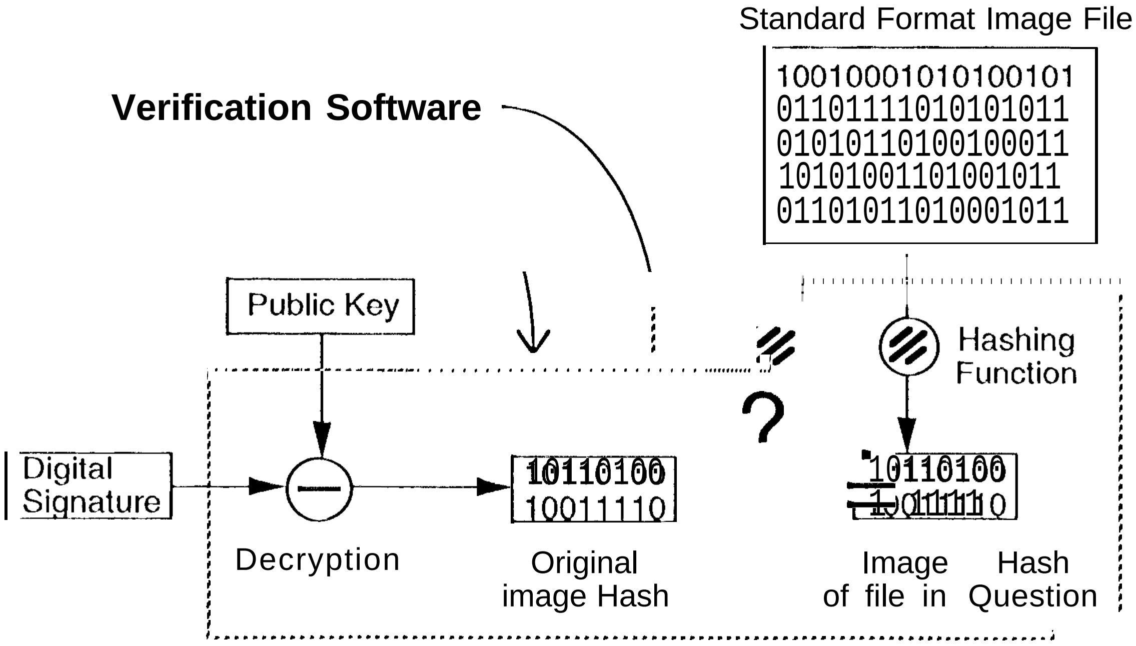
Step 1: When a single photo is taken, two files are produced: a standard digital image file, and an encrypted digital signature. The files can be stored on a variety of media, such as Kodak's Photo CD or the computer's mass storage device. The image can then be accessed and used just as any other computer data.



Step 2: The Digital Signature is created by producing a complex checksum called a "hash", which is then encrypted using the private key embedded within the secure microprocessor. Attempting to forge this signature without knowledge of the private key would take decades using today's supercomputer technologies.



Step 3: To authenticate the image, public domain verification software is run on a standard computer platform. The program takes as input the image file in question, the digital signature, and the camera's serial number (which doubles as its public key).



Step 4: The verification software computes its own hash of the image in question, and-compares it to the original hash which has been decrypted using the public key. If the image in question has not been manipulated, the decrypted digital signature and the program's own hashing function will match, resulting in an authentication. If even a single bit is different, the two hashes will not even closely match, yielding an authentication failure,

Bibliography

[1] "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithm", IEEE Transactions on Information Theory, Vol. IT-31 no. 4, (July 1985), Taher ElGamal, pp. **47?)-81** .

[2] "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, VOJ. 21 no. 2 (February, 1978), R.L. Rivest, A. Shamir, L. Adleman, pp. 120-26.

[3] "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. IT-22 no. 6 (November, 1976), Whitfield Diffie and Marlin E. Hellman, pp. 644-54.

[4] "The Proposal for a U.S. Standard for Digital Signature Encoding", IEEE Spectrum, August, 1992, Dennis K. Branstad, pp. 30.

[5] **"8051** Tackles Secure Smart-card Applications", EDN, December 10, 1992, pp. 46-48.

[6] Kodak Photo-CD ROM standard reference.

[7] "Photography by the Numbers", BYTE, January 1993, Howard Eglowstein, pp. 241-244.