Penggunaan Tanda Tangan Digital untuk Menjamin Keabsahan Swafoto KTP

Fransiskus Febryan Suryawan - 13519124
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail: franfebryan@gmail.com

***Abstrak*—Penggunaan swafoto KTP sebagai bagian dari proses verifikasi identitas sekarang menjadi hal yang umum dilakukan. Bahkan, proses tersebut diharuskan menurut undang-undang, yaitu sebagai proses mengenali pelanggan. Namun, muncul keraguan dalam masyarakat karena banyaknya kasus penyalahgunaan swafoto KTP. Tanda tangan digital yang disematkan dalam foto dapat digunakan untuk menyangkal penggunaan swafoto KTP yang tidak diinginkan.**

Keywords— DSA; Know Your Customer, swafoto KTP; tanda tangan digital

I. Pendahuluan

Penggunaan swafoto KTP untuk verifikasi identitas merupakan kewajiban menurut undang-undang, seperti tercantum dalam [1]. Kewajiban tersebut adalah bagian dari prosedur wajib *Know Your Customer* (Mengetahui Pelanggan Anda). Namun, banyak terjadi kasus penyalahgunaan swafoto KTP. Hal tersebut dapat terjadi karena foto yang dikirimkan oleh pengguna kemudian digunakan kembali oleh pihak tak berwenang. Pengguna tidak dapat menyangkal penggunaan tak berwenang tersebut karena pengguna tidak dapat membuktikan bahwa pengirim foto adalah pihak ketiga.

Salah satu cara untuk menjamin kepemilikan foto dan penggunaannya adalah dengan menggunakan tanda tangan digital. Namun, apabila tanda tangan dilakukan terhadap berkas foto tanpa tambahan data, maka pihak ketiga tetap dapat menggunakan foto yang sama untuk digunakan kembali. Informasi tambahan seperti tanggal penggunaan dan tujuan foto dapat dimasukkan untuk memperkuat bukti yang dimiliki pengguna untuk menyangkal penggunaan yang tidak diinginkan.

Proses tanda tangan digital menggunakan *hash* atau *message digest* dari data untuk melakukan tanda tangan, sesuai dengan standar untuk tanda tangan digital [2]. Hal tersebut menjamin integritas data yang ditandatangani. Akibatnya, tidak ada data yang dapat ditambahkan ke data awal, termasuk tanda tangan. Umumnya, tanda tangan digital merupakan berkas yang dapat dipisahkan dari berkas utama, sehingga hal tersebut bukan masalah. Namun, standar JPEG tidak mendukung tanda tangan digital. Salah satu alternatif adalah untuk menyisipkan tanda tangan sebagai metadata, kemudian metadata tersebut dihapus saat tanda tangan akan diverifikasi.

II. Teori Dasar

A. Format JPEG

JPEG merupakan format paling umum untuk menyimpan data berupa foto. Format berkas ini memungkinkan foto untuk disimpan secara terkompres [3]. Terdapat dua jenis kompresi yang didefinisikan dalam standar [3], yakni *lossy* dan *lossless*. Jenis yang umum digunakan adalah jenis *lossy* yang menggunakan *discrete cosine transform*(DCT) untuk melakukan kompresi. Proses kompresi yang dilalui akan menghilangkan sebagian data, sehingga data yang dihasilkan berukuran lebih kecil. Karena proses kompresi terjadi dalam ranah ruang-frekuensi, maka perubahan tidak akan tampak kasat mata apabila dilihat sekilas.

Format berkas JFIF (JPEG File Interchange Format) adalah perluasan dari format JPEG. Dalam format JFIF, metadata foto disimpan bersamaan dalam berkas foto. Metadata dalam JFIF dapat menyimpan beragam informasi, seperti *colorspace* yang digunakan, jenis kamera, dan sebagainya. Metadata yang ada diidentifikasi dengan 2 byte tag, diawali nilai byte 0xFF dan dilanjutkan oleh nilai byte yang menunjukkan jenis penanda.

Jenis format berkas yang lain adalah EXIF (Exchangeable Image File Format). Format berkas ini serupa dengan format JFIF. Format berkas EXIF tidak kompatibel dengan JFIF, namun EXIF dapat disisipkan dalam JFIF untuk menambahkan metadata. Selain itu, EXIF juga memperbolehkan urutan byte "Intel" (diawali byte 0x4949) atau "Motorola" (diawali byte 0x4D4D), seperti dijelaskan dalam [4]. Format JFIF secara umum lebih sering digunakan dalam pengiriman berkas, sedangan berkas EXIF adalah berkas yang lebih umum dihasilkan oleh kamera digital.

Terdapat byte-byte penanda (*marker*) yang digunakan oleh format JFIF untuk menandakan daerah informasi. Penanda yang selalu ada dalam JPEG adalah nilai 0xFFD8 (*Start of Image*, SOI) dan nilai 0xFFD9 (*End of Image*, EOI). Di antara SOI dan EOI, terdapat berbagai penanda serta data foto dalam JPEG yang disimpan. Penanda yang umumnya muncul pertama kali setelah SOI adalah 0xFFE0 (APP0, digunakan oleh JFIF) atau 0xFFE1 (APP1, digunakan oleh EXIF). Format JFIF tidak memberikan banyak keleluasaan dalam metadata. Oleh karena itu, umumnya JFIF juga menampung metadata dalam format EXIF.

Salah satu penanda yang dapat menampung data dengan panjang sembarang adalah *UserComment* dengan tag 0x9286. Data yang ditampung oleh tag ini harus dimulai dengan 8 byte yang menandakan kode karakter yang digunakan (*encoding*), diikuti oleh *string* yang disisipkan. String yang disisipkan tidak perlu diakhiri oleh *null terminator* (0x00).

B. Kriptografi

Menurut [5], kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Kriptografi dapat memberikan aspek-aspek keamanan sebagai berikut:

- Kerahasiaan (*confidentiality*), yaitu aspek keamanan yang menjaga pesan agar tidak dapat dibaca oleh pihak tak berwenang.
- Integritas Data (*data integrity*), yaitu aspek yang menjamin keaslian/keutuhan data. Aspek ini menjamin bahwa data yang diterima tidak berubah saat pengiriman.
- Otentikasi (*authentication*), yaitu aspek yang berhubungan dengan identifikasi. Identifikasi dapat terkait pihak yang sedang berkomunikasi maupun terkait pengirim dari pesan.
- Nirpenyangkalan (*non-repudiation*), yaitu aspek yang mencegah terjadinya penyangkalan yang dapat dilakukan oleh pengirim pesan maupun penerima pesan.

Sebagian besar teknik-teknik kriptografi modern didasarkan pada teori-teori matematika. Teknik kriptografi modern secara umum menggunakan permasalahan matematis yang sulit untuk dipecahkan. Selain itu, kriptografi modern juga terkait erat dengan ilmu komputer.

Untuk mencapai aspek kerahasiaan, digunakan penyandian cipherteks. Penyandian dilakukan dengan cara memetakan pesan asal kepada suatu cipherteks (selanjutnya disebut enkripsi). Kemudian, cipherteks dapat dikembalikan dengan memetakan kembali cipherteks ke pesan asal (selanjutnya disebut dekripsi). Cara melakukan penyandian ini beragam, tergantung algoritma dan teknik yang digunakan.

Teknik paling sederhana dalam kriptografi untuk melakukan penyandian cipherteks adalah kriptografi kunci simetri. Dalam kriptografi kunci simetri, kunci yang digunakan untuk melakukan enkripsi sama dengan kunci yang digunakan untuk melakukan dekripsi. Kelemahan dari teknik ini adalah perlu adanya saluran komunikasi aman untuk bertukar kunci.

C. Kriptografi Kunci-Publik

Kriptografi kunci-publik adalah teknik dalam kriptografi yang menggunakan dua kunci berbeda dalam enkripsi dan dekripsi. Salah satu kunci, umumnya disebut sebagai kunci publik, digunakan sebagai kunci untuk enkripsi. Kunci lain yang disebut sebagai kunci privat kemudian dapat digunakan untuk mendekripsi pesan. Kunci yang digunakan untuk melakukan dekripsi harus berasal dari pasangan kunci yang sesuai untuk mendapatkan pesan awal. Sesuai dengan namanya, kunci publik adalah kunci yang dapat disebarkan kepada pihak lain. Kunci privat bersifat rahasia, sehingga tidak boleh diketahui oleh pihak lain.

Skema kriptografi ini memungkinkan dua pihak untuk bertukar pesan melalui saluran yang tidak aman tanpa perlu menyetujui kunci tertentu. Pengirim hanya perlu mengetahui kunci publik dari penerima untuk melakukan enkripsi yang ditujukan pada penerima. Dengan demikian, aspek kerahasiaan dapat dijamin.

D. Hash

Fungsi hash adalah fungsi yang memetakan pesan dengan panjang sembarang ke suatu *bit string* dengan panjang tetap yang disebut sebagai *message digest*. Fungsi hash bersifat satu arah, artinya *message digest* tidak dapat dikembalikan menjadi pesan semula. Selain itu, fungsi hash juga tidak menggunakan kunci dalam prosesnya. Maka fungsi hash berbeda dengan fungsi enkripsi.

Sebuah fungsi hash h harus memiliki setidaknya sifat-sifat berikut [6]:

- *Compression*: h memetakan masukan dengan panjang bit sembarang pada suatu keluaran dengan panjang bit tertentu.
- *Ease of computation*: diberikan suatu masukan x, mudah untuk menghitung $h(x)$.

Sifat-sifat yang sebaiknya dimiliki oleh fungsi hash sesuai dengan [6] adalah:

- *Collision resistance*, artinya sukar untuk mencari dua pesan berbeda yang memiliki *message digest* yang sama
- *Preimage resistance*, artinya sukar untuk mencari pesan awal jika diketahui *message digest*-nya
- *Second preimage resistance*, artinya apabila diberikan sebuah pesan, sukar untuk mencari pesan lain yang memiliki *message digest* yang sama dengan pesan pertama.

Pembangunan fungsi hash umumnya menggunakan blok-blok berukuran tertentu. Pesan dipecah menjadi blok, kemudian setiap blok dimasukkan kedalam fungsi kompresi secara berantai. Hasil dari fungsi kompresi selanjutnya digunakan sebagai bagian dari masukan fungsi kompresi untuk iterasi selanjutnya. Umumnya, iterasi pertama akan menggunakan masukan tambahan berupa *Initialization Vector* (IV) agar fungsi kompresi serupa untuk seluruh blok pesan.

Aspek keamanan yang dapat diberikan oleh sebuah fungsi hash adalah integritas data. Nilai *message digest* dapat dikirimkan secara terpisah dari data untuk menjamin integritas data. Apabila *message digest* dari data yang diterima berbeda dengan *message digest* yang diterima, maka terdapat perubahan dalam data.

E. Tanda Tangan Digital

Tanda tangan digital adalah sebuah potongan informasi yang menghubungkan suatu data dengan pihak yang memiliki atau mengeluarkan data tersebut. Pembuatan tanda tangan digital menggunakan fungsi hash yang sudah ditentukan untuk menghasilkan *message digest* dari data yang akan ditandatangan. Kemudian dari *message digest* tersebut akan

dibentuk sebuah tanda tangan dengan algoritma bakuan DSA(*Digital Signing Algorithm*). Algoritma tersebut bekerja dengan konsep kriptografi kunci-publik. Parameter dalam DSA adalah:

- p, bilangan prima dengan panjang L bit.
- q, pembagi prima dari $(p-1)$ dengan panjang N bit.
- g, generator dengan $\mathrm{g} = h^{(p-1)/q} \bmod \mathrm{p}$, $h < p-1$ sedemikian sehingga $h^{(p-1)/q}\ mod\ p > 1$.
- x, bilangan acak kurang dari q
- y, kunci publik dengan $y = g^x\ mod\ p$
- k, nilai acak yang unik untuk setiap pesan

Pilihan nilai L dan N yang diberikan oleh DSS adalah sebagai berikut:

- L = 1024, N = 160
- L = 2048, N = 224
- L = 2048, N = 256
- L = 3072, N = 256

Parameter p, q, g, dan y merupakan parameter publik, yang dapat diketahui oleh pihak-pihak yang akan menerima pesan. Sedangkan parameter x adalah parameter privat, yang hanya boleh diketahui oleh pengirim pesan.

Pembangkitan tanda tangan digital dalam DSA akan menghasilkan dua buah parameter, r dan s. Kedua parameter tersebut adalah tanda tangan digital, dan dapat dihitung sebagai berikut:

$$r = (g^k\ mod\ p)\ mod\ q$$

$$s = \left(k^{-1}(\mathrm{Hash}(M) + xr)\right) \bmod q$$

Dengan Hash adalah fungsi hash yang dipilih. Fungsi hash yang digunakan dalam bakuan DSA Parameter r dan s yang dihasilkan dapat disisipkan dalam pesan. Penerima kemudian dapat memverifikasi bahwa pesan yang ditandatangan sesuai dengan menghitung nilai-nilai berikut:

$$w = s^{-1} \bmod q$$

$$u_1 = (\mathrm{Hash}(M)w) \bmod q$$

$$u_2 = (rw) \bmod q$$

$$v = \left((g^{u_1} y^{u_2}) \bmod p\right) \bmod q$$

Dengan Hash adalah fungsi hash yang dipilih. Apabila ditemukan $v = r$, maka tanda tangan dapat dinyatakan sah. Selain itu, tanda tangan dinyatakan tidak sah dan ditolak.

Selain algoritma bakuan DSA, tanda tangan digital dapat dibentuk menggunakan gabungan dari fungsi hash dan fungsi kriptografi kunci-publik. Fungsi kriptografi kunci-publik dapat digunakan untuk melakukan enkripsi terhadap *message digest*, kemudian penerima dapat membandingkan *message digest* dari pesan yang diterima dengan *message digest* hasil dekripsi untuk menentukan keaslian pesan.

III. Skema Penandatanganan

Alur pembangkitan parameter-parameter dalam DSA dapat dilihat pada Fig. 1. Kemudian, tanda tangan untuk berkas swafoto dapat dibuat sesuai dengan alur pada Fig. 2. Penandatanganan dilakukan dengan menyisipkan tujuan serta waktu penandatanganan dimulai dalam foto. Hal tersebut digunakan untuk mencegah penggunaan foto yang valid pada pihak yang tidak seharusnya. Kemudian, alur verifikasi swafoto dapat dilihat pada Fig. 3. Karena verifikasi membutuhkan data yang sama dengan saat pembuatan, maka tanda tangan dihapus sementara dari berkas foto.

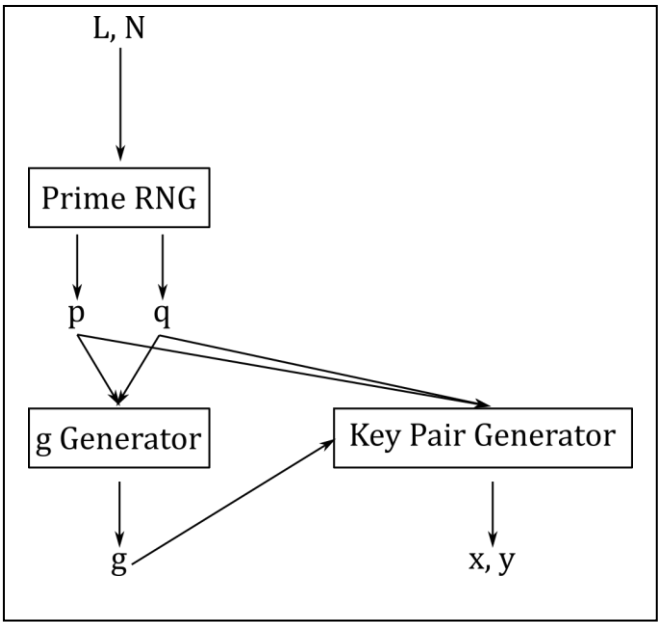

Fig. 1. Alur pembangkitan parameter DSA

Skema ini menggunakan SHA-256 sebagai fungsi hash. Kemudian, pasangan (L, N) yang akan digunakan dalam skema ini adalah $(2048, 256)$. Fungsi SHA-256 dipilih sebagai fungsi hash karena fungsi ini mengeluarkan 256 bit sebagai message digest. Walaupun *User Comment* dalam EXIF dapat berisi teks dengan panjang sembarang, namun ukuran teks yang terlalu panjang akan merugikan sebab akan lebih banyak data yang harus dikirimkan.

Kompleksitas dalam pendistribusian dan penjaminan kepemilikan kunci publik tidak ditampilkan dalam skema ini. Penerima diasumsikan memiliki kunci publik dari pengirim, dan mempercayai bahwa kunci publik tersebut bukanlah kunci publik dari pihak ketiga yang berusaha meniru pengirim. Skema untuk pendistribusian kunci public yang umumnya dilakukan adalah *Public Key Infrastructure*(PKI), namun skema tersebut membutuhkan suatu entitas pihak ketiga yang dipercaya untuk menyimpan dan mendistribusikan kunci publik. Skema lain yang dapat digunakan untuk mendistribusikan kunci public beserta identitasnya adalah *web-of-trust* (jaringan kepercayaan), yang digunakan dalam *Pretty Good Privacy*(PGP).

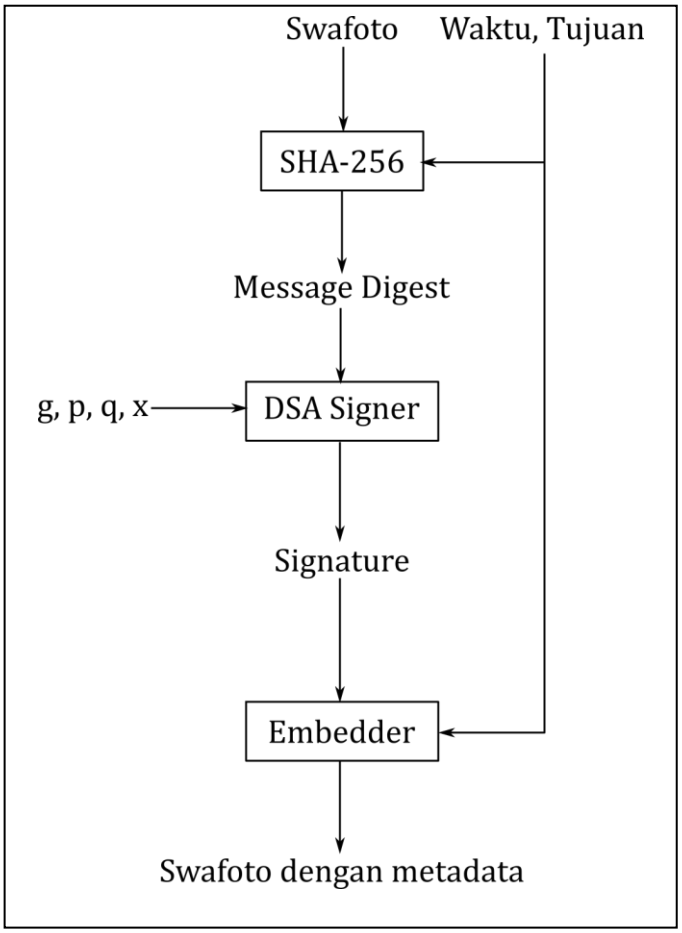

Fig. 2. Alur penandatanganan swafoto

Pembangkitan parameter publik dan privat dalam DSA dilakukan oleh pengirim. Pembangkitan parameter p, q, g, x, y dapat dilakukan satu kali untuk satu pengirim, sedangkan parameter k harus dibangkitkan secara acak setiap kali ada berkas baru yang akan ditandatangan. Kemudian, pengirim dapat mengirimkan parameter publik kepada penerima. Penerima dapat memverifikasi tanda tangan digital untuk memastikan keabsahannya. Selain itu, terdapat metadata berupa waktu tanda tangan dilakukan, serta tujuan dari swafoto. Metadata tujuan merupakan metadata yang dapat membatasi penggunaan swafoto tersebut hanya untuk layanan tertentu. Metadata waktu dapat membatasi penggunaan swafoto dalam jangka waktu tertentu saja.

Apabila terjadi penggunaan swafoto oleh pihak ketiga yang tidak bertanggungjawab, maka penggunaan swafoto tersebut dapat disangkal berdasarkan metadata tujuan. Isi dari metadata tujuan akan berbeda dengan layanan yang didaftarkan oleh pihak ketiga tersebut. Akibatnya, swafoto yang dikirimkan dapat dikatakan tidak sah untuk digunakan dalam layanan tersebut.

Pihak yang memverifikasi tanda tangan digital sebaiknya adalah pihak penerima, yaitu layanan. Dengan demikian, penggunaan swafoto yang tidak valid dapat segera diabaikan. Namun, apabila pihak layanan tidak memverifikasi hal tersebut terlebih dahulu, pengguna dapat melakukan penyangkalan dengan membuktikan metadata yang ada dan tanda tangan digital yang sah.

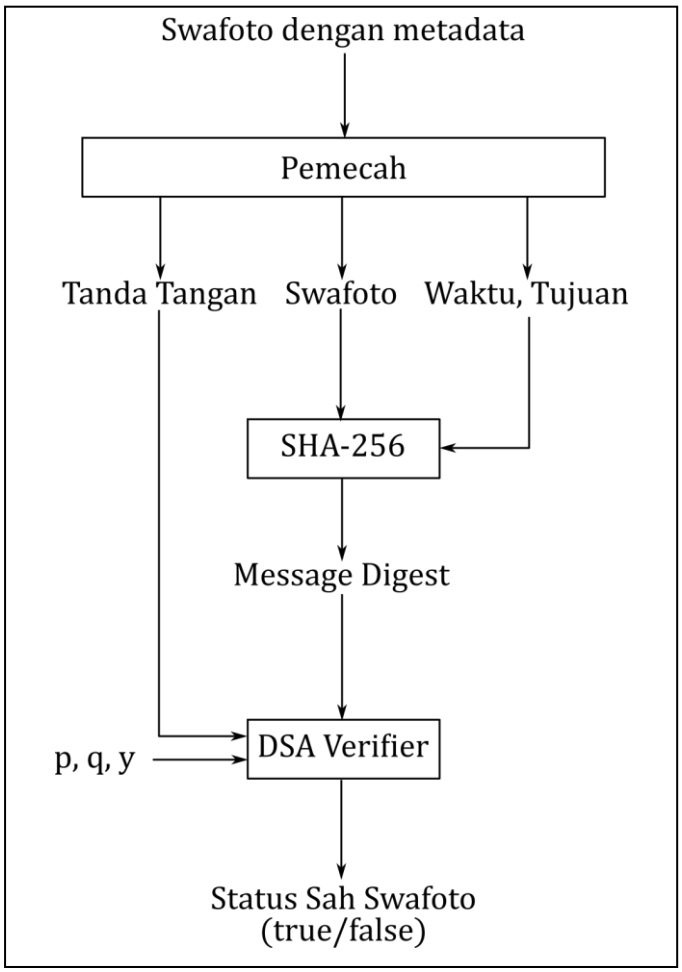

Fig. 3. Alur verifikasi swafoto

Tanda tangan digital ini juga dapat digunakan untuk melindungi swafoto dari perubahan yang tak diinginkan. Apabila terdapat pihak yang mencoba melakukan manipulasi terhadap foto, tanda tangan akan menjadi tidak sah. Hal ini sesuai dengan prinsip yang diberikan oleh tanda tangan digital, yakni integritas data.

IV. Implementasi dan Uji Coba

Implementasi dibagi menjadi beberapa bagian, yaitu bagian hash, bagian tanda tangan dan verifikasi menggunakan DSA, bagian penyisipan tanda tangan, dan bagian pemisahan tanda tangan. Untuk bagian hash, dilakukan implementasi fungsi SHA-256. Bagian tanda tangan berisi fungsi *sign* dan *verify* dari DSA. Bagian penyisipan tanda tangan melakukan penyisipan kedalam tag *UserComment* baru dari EXIF. Bagian pemisahan tanda tangan mengambil tanda tangan serta metadata lain dari *UserComment*, kemudian menghapus tag *UserComment*.

Implementasi dibuat dalam bahasa pemrograman Python 3.9. Bentuk metadata yang disisipkan dalam *UserComment* adalah nilai-nilai r, s, waktu penandatanganan, serta tujuan.

Keempat nilai tersebut dimasukkan secara berurutan sebagai *string* karakter ASCII yang dipisahkan oleh koma. Waktu penandatanganan disimpan sebagai *string* sesuai dengan standar ISO 8601. Tujuan adalah masukan dari pengguna yang menunjukkan pihak yang seharusnya menerima swafoto terkait.

Untuk pengujian, sebuah foto akan ditandatangani secara digital. Foto yang menjadi swafoto KTP *dummy* dapat dilihat pada Fig. 4. Pada awalnya, bagian tag *UserComment* dari foto tersebut kosong, sesuai dengan Fig. 5.

Fig. 4. Contoh swafoto KTP

```
[dir: D:\edustuff\I\IF4020\tugas\makalah]
[franf@ASTERIA]$ exiftool -UserComment .\tes_foto.jpg
[dir: D:\edustuff\I\IF4020\tugas\makalah]
[franf@ASTERIA]$
```

Fig. 5. Hasil query tag UserComment pada gambar asli

Kemudian, parameter DSA dibangkitkan dan disimpan dalam berkas bernama *pubkey* untuk parameter publik dan *privkey* untuk parameter privat. Setelah parameter DSA dibangkitkan, maka tanda tangan dapat dihitung. Perhitungan tanda tangan dilakukan terhadap berkas swafoto ditambah dengan waktu penandatanganan dan tujuan. Setelahnya, tanda tangan akan disisipkan dalam tag *UserComment*. Dalam Fig. 6 ditampilkan penandatanganan foto dan query terhadap bagian *UserComment* menggunakan exiftool. Namun, exiftool tidak dapat mendeteksi tag *UserComment* yang ditambahkan dengan baik.

```
[dir: D:\edustuff\I\IF4020\tugas\makalah]
[franf@ASTERIA]$ python sign.py tes_foto.jpg_original coba1 tes_signed.jpg
[dir: D:\edustuff\I\IF4020\tugas\makalah]
[franf@ASTERIA]$ exiftool .\tes_signed.jpg -UserComment
Warning: [minor] Skipped unknown 18 bytes after JPEG APP1 segment - ./tes_signed.jpg
[dir: D:\edustuff\I\IF4020\tugas\makalah]
```

Fig. 6. Hasil query tag UserComment pada gambar setelah ditandatangan

Penyisipan tanda tangan tidak menyebabkan kerusakan apapun pada berkas foto. Berkas foto yang disisipkan tanda tangan serta metadata lain dapat dilihat pada Fig. 7. Berkas foto tersebut akan lolos pengujian tanda tangan seperti pada Fig. 8.

Fig. 7. Swafoto yang telah disisipkan tanda tangan

```
[dir: D:\edustuff\I\IF4020\tugas\makalah]
[franf@ASTERIA]$ python verify.py tes_signed.jpg
Tanggal penandatanganan: 2021-12-11T23:11:21.358253, Tujuan: coba1
Status verifikasi: Berhasil
```

Fig. 8. Pengujian metadata pada swafoto

Karena berkas swafoto tidak diubah, maka hasil dari pengujian tanda tangan adalah sah. Metadata lain, seperti tanggal penandatanganan dan tujuan dapat digunakan untuk menerima atau menolak, apabila tanggal penandatanganan terlalu jauh dari penggunaan ataupun tujuan yang tidak tepat. Apabila berkas diubah, maka hasil verifikasi dapat berubah menjadi tidak sah. Hal ini dapat dilihat pada Fig. 9.

```
[dir: D:\edustuff\I\IF4020\tugas\makalah]
[franf@ASTERIA]$ python verify.py tes_signed_invalid.jpg
Tanggal penandatanganan: 2021-12-11T23:24:58.781758, Tujuan: coba1
Status verifikasi: Gagal
```

Fig. 9. Pengujian berkas yang tidak sah

V. KESIMPULAN DAN SARAN

Penggunaan tanda tangan digital dapat mengurangi penggunaan swafoto KTP yang tidak sah. Dengan demikian, kasus penggunaan identitas oleh pihak yang tak berwenang dapat dicegah. Namun, penggunaan tanda tangan digital dapat meningkatkan kompleksitas serta penggunaan memori. Selain itu, penggunaan tanda tangan digital juga masih belum umum untuk swafoto, sehingga akan sulit untuk mengadopsi hal ini.

Implementasi algoritma DSA dan SHA mungkin dapat dilakukan dengan lebih efisien, sehingga waktu yang digunakan untuk membangkitkan tanda tangan digital dapat dikurangi. Selain itu, penggunaan pustaka pihak ketiga dapat mempercepat pembangkitan kunci, karena pembangkitan kunci cukup kompleks untuk dilakukan dalam Python. Pengaksesan metadata EXIF juga cukup kompleks, dan cukup sulit untuk membuat berkas foto yang identik namun dengan mengatur metadata dalam EXIF.

UCAPAN TERIMAKASIH

Terima kasih penulis ucapkan bagi bapak Dr. Ir. Rinaldi Munir, M.T. selaku dosen pengajar mata kuliah IF4020 Kriptografi Tahun Ajaran 2021/2022. Berbagai ilmu dan pengalaman telah dituangkan dalam materi perkuliahan hingga penulis mampu menuliskan makalah ini.

REFERENSI

[1] *Peraturan Bank Indonesia No. 3/10/PBI/2021 Tentang Penerapan Prinsip Mengenal Nasabah*, 2021.

[2] National Institute of Standards and Technology, "Digital Signature Standard (DSS)".

[3] The International Telegraph and Telephone Consultative Committee, *Information Technology - Digital Compression and Coding of Continuous-Tone Still Images - Requirements and Guidelines*, 1993.

[4] T. Tachibanaya, "Description of Exif file format," 1999.

[5] B. Schneier, Applied Cryptography, 2 ed., John Wiley & Sons, 1996.

[6] P. v. O. S. V. Alfred Menezes, Handbook of Applied Cryptography, CRC Press, 1996.

[7] R. Munir, Kriptografi, ITB Press.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 16 Desember 2021

Fransiskus Febryan Suryawan