Vol. 4 No. 1 – Tahun 2025
Indonesian Journal Computer Science
ISSN: 2829-3819

Skema Anti Pemalsuan Produk Berbahan Kulit Buaya Berbasis *dhash*

Genta Nazwar Tarempa[1], Yuki Rizki Adam Nugraha[2], Andi Nur Rachman[3]
Universitas Siliwangi[123]
genta.tarempa@unsil.ac.id[1], yuki@unsil.ac.id[2], andy.rachman@unsil.ac.id[3]

Diterima	Direvisi	Disetujui
(10-04-2025)	(16-04-2025)	(21-04-2025)

Abstrak - Kulit buaya memiliki nilai ekonomis yang sangat tinggi dan sering digunakan sebagai bahan pembuatan produk-produk *"branded"*. Beberapa alasannya yaitu kelangkaan dan ketatnya regulasi dalam penggunaan kulit buaya. Selain itu keunikan dan kualitas kulit buaya, menjadikannya lebih eksklusif sehingga meningkatkan nilai jual produk. Dengan fakta ini, banyak pihak yang ingin memalsukan produk berbahan kulit buaya demi mencari keuntungan yang besar. Pemalsu akan memanfaatkan ketidaktahuan pembeli mengenai produk yang asli sebab terkadang cukup sulit untuk membedakan produk asli ataupun palsu, sehingga perlu ada penanda yang dapat membedakannya. Salah satu penanda yang sering digunakan adalah *tag NFC*. *Tag NFC* ini akan menyimpan informasi mengenai produk asli, sehingga pembeli dapat melakukan validasi keaslian produk hanya dengan memindai *tag* NFC. Namun, masalah lain muncul apabila *tag NFC* ini diterapkan kembali pada produk palsu sehingga produk palsu seolah-olah merupakan produk asli. Untuk mengatasi masalah ini, kami mengembangkan skema anti pemalsuan produk berbahan kulit buaya dengan memanfaatkan *tag NFC*, kriptografi kunci publik dan *difference hash* (*dHash*). Pada skema ini, *dHash* berfungsi untuk menyimpan informasi berupa korelasi antara produk dan data dalam *tag NFC*. Untuk mengetahui bahwa skema ini dapat mendeteksi dan tahan terhadap serangan pemalsuan maka akan dievaluasi dengan tiga skenario serangan, yaitu *tag NFC* yang dimodifikasi, dikloning, dan diterapkan kembali. Hasilnya, skema ini terbukti mampu mendeteksi dan tahan terhadap serangan pemalsuan. Selain itu skema ini juga membantu instansi terkait dalam memantau pemanfaatan kulit buaya untuk produk-produk komersial secara legal guna menjaga populasi buaya, karena skema ini melibatkan instansi sebagai pihak ketiga dalam otentikasi bahan kulit buaya.

Kata Kunci : skema anti pemalsuan, *dhash*, kulit buaya, *nfc*

Abstract *- Crocodile leather has a high economic value due to its scarcity, strict regulations, and unique texture, making it a target for counterfeiters seeking high profits. Buyers often struggle to distinguish genuine from fake products, prompting the use of markers such as NFC tags to verify authenticity. However, NFC tags can be exploited by reapplication them to counterfeit goods, making fake products appear authentic. We propose an anti-counterfeiting scheme using NFC tags, public key cryptography, and difference hash (dHash) to address this. The dHash algorithm links visual features of the product to the data stored in the NFC tag, enabling image-based authentication. The scheme also involves real-time online authentication and integrates with a central server managed by authorized agencies to monitor legal crocodile leather usage. We evaluated the scheme against three attack scenarios: tag modification, cloning, and reapplication. Results show that the system effectively detects unauthorized changes through digital signature verification, identifies tag duplication using unique tag IDs, and prevents tag reapplication by comparing hash values and tag reading counters. Additionally, the system supports regulatory agencies in tracking the legal use of crocodile leather in the supply chain. This research demonstrates that the proposed scheme is effective for real-time authentication and protection against counterfeit crocodile leather products while supporting sustainability and conservation efforts.*

Keywords: anti-counterfeiting, dhash, crocodile leather, nfc

I. PENDAHULUAN

Kulit buaya adalah salah satu bahan pembuatan produk-produk eksklusif yang banyak diproduksi oleh merek-merek ternama. Produk berbahan kulit buaya memiliki nilai ekonomi yang sangat tinggi. Hal ini disebabkan oleh beberapa hal, antara lain:

1. Regulasi pemanfaatan kulit buaya sebagai bahan baku suatu produk sangat ketat. Hal ini diakibatkan karena populasi buaya di alam liar cukup terbatas sehingga menyebabkan kelangkaan pasokan kulit buaya (*demand* yang lebih tinggi dibanding *supply*). Andaipun kulit buaya diperoleh dari penangkaran maka biaya budidaya dan pemeliharaannya cukup tinggi sebab

dibutuhkan waktu sampai beberapa tahun agar buaya siap untuk diambil kulitnya. Selain itu, pengolahan kulit buaya memerlukan proses penyamakan khusus untuk memastikan kulit dapat tahan lama dan memiliki kualitas yang tinggi. Proses ini dapat menghabiskan waktu pengerjaan yang panjang dan membutuhkan keahlian yang tinggi dari pekerjanya.

2. Kualitas kulit buaya yang kuat dan tahan lama serta keunikan pada tekstur dan pola sisik alami yang jarang dimiliki oleh kulit hewan lainnya, sehingga produk kulit buaya tidak bisa ditiru. Hal inilah yang membuat setiap produk menjadi eksklusif.

Hal-hal tersebut di atas berdampak pada nilai jual produk berbahan kulit buaya menjadi meningkat dan mahal. Hal ini mengundang banyak pihak melakukan pemalsuan produk demi mencari keuntungan yang besar. Pemalsu akan berusaha membuat produk yang mirip dengan produk aslinya dan menjualnya dengan nilai yang lebih rendah dari aslinya. Walaupun begitu pemalsu masih tetap memperoleh margin keuntungan yang tinggi.

Dengan memanfaatkan ketidaktahuan pembeli akan produk yang asli, pemalsu membuat produk yang sedemikian rupa mirip dengan produk asli yang terkadang memang cukup sulit untuk bisa dibedakan. Sehingga perlu ada penanda yang dapat digunakan untuk membedakan produk asli dan produk palsu atau tiruan. (Blankenburg et al., 2015)

Salah satu penanda yang untuk membedakan produk asli atau palsu adalah penggunaan *tag NFC*. *Tag NFC* ini akan menyimpan informasi mengenai produk asli, sehingga pada saat produk dibeli dan *tag NFC* dipindai, maka pembeli akan mudah memperoleh validasi tentang keaslian produknya.

Namun masalah lain muncul jika pemalsu menerapkan *tag NFC* sendiri atau mungkin menerapkan kembali *tag NFC* dari produk asli ke produk palsu yang membuat produk palsu ini seolah-olah adalah produk asli. (Bulusu & Alzahrani, n.d.) (Saeed et al., 2013)

Dalam studi ini, pendekatan yang diusulkan untuk mengatasi masalah yang dihadapi adalah melalui skema Deteksi Penerapan Ulang Tag (*Tag Re-application Detection*, *TRD*) yang telah dikembangkan sebelumnya. Skema ini memanfaatkan teknologi *NFC* dengan menambahkan fitur *Counter read-only*, di mana nilai *Counter* akan bertambah setiap kali tag dibaca. Selain itu, skema ini juga mengintegrasikan kriptografi kunci publik (Lin, 2023), pemanfaatan *difference hash* (dHash) serta protokol otentikasi online. Protokol ini digunakan untuk setiap proses otentikasi baik pada saat produk berada dalam rantai pasokan seperti distributor, toko, atau re-*seller* maupun setelah produk ada di tangan pembeli. Protokol ini menghubungkan seluruh *node* dengan *server* otentikasi produsen. *Server* otentikasi menyimpan *database* mengenai rincian produk, termasuk jumlah *tag NFC* tersebut telah dibaca selama berada dalam rantai pasokan. Selain itu, terdapat juga otentikasi kulit buaya yang dilakukan oleh produsen pada saat menerima bahan baku kulit buaya dari pemasok. Otentikasi ini dilakukan oleh produsen ke *server* otentikasi milik asosiasi untuk memastikan bahwa kulit buaya yang akan dioleh telah terdaftar dan legal.

Penelitian ini fokus pada produk-produk yang terbuat dari kulit buaya, seperti tas dan dompet, yang memiliki keunikan dalam corak dan motif kulitnya. Untuk itu, skema ini menggunakan *Perceptual Hash Function* (*PHF*), yakni *Difference Hash* (*dHash*), untuk membedakan corak dari setiap tas atau dompet kulit buaya yang ada (Samanta & Jain, 2021) (Monga & Evans, n.d.). Pemilihan *PHF* dalam skema ini didasarkan pada kemudahan implementasinya, jika dibandingkan dengan algoritma *machine learning* atau kecerdasan buatan yang lebih kompleks (Tarempa & Syalim, n.d.) (Farisa et al., 2016) (Naumenko, 2025). Selain itu, skema ini juga berperan dalam membantu instansi terkait memantau penggunaan kulit buaya secara ilegal, sehingga populasi buaya dapat tetap terjaga dengan baik.

Fitur-fitur yang dimiliki skema ini antara lain:

1. Seluruh proses otentikasi produk dilakukan secara *online* sehingga otentikasi berjalan dalam *real-time*.
2. Fitur *QR Code* pada produk untuk memperbarui status penjualan pada saat transaksi pembelian, sebagai langkah keamanan tambahan (Tiwari, 2017) (Warasart & Kuacharoen, n.d.) (Prabhu Shankar et al., 2024)
3. Proses otentikasi produk dengan memanfaatkan *difference hash* (*dHash*), sehingga menjadikannya lebih aman dan cepat.

II. METODOLOGI PENELITIAN

Skema anti pemalsuan produk berbahan baku kulit buaya memanfaatkan teknologi *NFC*, *QR Code*, dan algoritma *dHash*. Dalam pelaksanaan skema ini juga diperlukan kerja sama dengan asosiasi atau instansi terkait yang bertugas mengawasi kesesuaian data kulit buaya sehingga diharapkan dapat mencegah eksploitasi kulit buaya secara ilegal.

1. *Tag NFC* (*Near Field Communication*)

Tag NFC merupakan suatu teknologi komikasi nirkabel jarak dekat yang

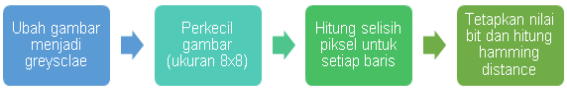
memungkinkan pertukaran data antara dua perangkat dengan cara ditempelkan satu sama lainnya. *Tag NFC* ini dibutuhkan dalam skema ini karena diperlukan pertukaran guna melakukan proses verifikasi atas keaslian produk. (Coskun et al., 2013)
Setiap produk akan dilengkapi dengan *tag NFC* yang menyimpan informasi detail, termasuk nomor seri produk, tipe dan warna, tanggal produksi, serta nama atau inisial produsen. Selain itu, informasi awal terkait kulit buaya dari pemasok dan nomor registrasinya juga akan disertakan. Sistem ini memanfaatkan tag yang memiliki fitur *NFC Read Counter* atau *ASCII Mirroring*, yang dapat menghitung berapa kali tag telah dibaca. Nilai *counter* ini akan bertambah secara otomatis setiap kali tag dibaca dan tidak bisa diubah atau ditimpa (hanya dapat dibaca). Tag ini juga dilengkapi dengan nomor seri *read-only* yang unik sebagai identitas *Tag* (*TID*).

2. *QR Code* (*Quick Response Code*)

QR Code adalah kode matriks yang dapat menyimpan banyak data serta dibaca dengan cepat menggunakan perangkat telepon pintar (Sutheebanjard & Premchaiswadi, n.d.). Dalam skema ini akan dimanfaatkan sebagai fitur keamanan tambahan yang akan dibaca oleh distributor / *re-seller* pada saat produk berhasil terjual. Pembacaan *QR Code* akan memicu perubahan data status penjualan dari sebelumnya berstatus "Belum Terjual" menjadi "*Sold*" atau terjual.

3. *Difference Hash* (*dHash*)

dHash adalah salah satu algoritma *Perceptual Hash Function* yang digunakan untuk menemukan kemiripan suatu gambar (Fei et al., 2017). Dengan kata lain, *dHash* merupakan *hash* visual yang tidak membutuhkan kemiripan yang tepat demi menemukan gambar yang mirip dengan tetap menjaga integritas gambar asli (tidak mengubah gambar asli) (Fei et al., 2017). *dHash* menghasilkan *hash* dengan menghitung perbedaan *hash* gambar (*hamming distance*) berdasarkan perubahan gradien warna antara piksel yang berdekatan dalam matriks gambar (Bookstein et al., 2002) (McKeown, 2025) (Santos et al., 2024). *dHash* menghasilkan nilai *hash* yang tahan terhadap penskalaan gambar, serta perubahan warna, kecerahan, dan rasio aspek. Salah satu kelebihan dHash ini adalah prosesnya yang sangat cepat.
Berikut adalah ringkasan algoritma *dHash*:

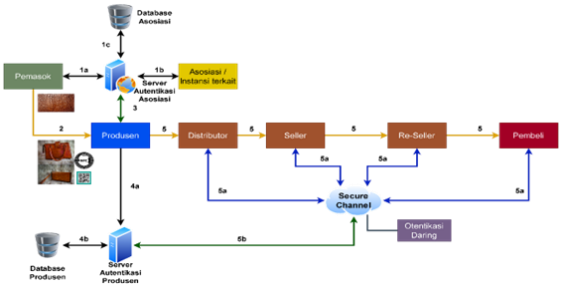


Sumber : Penelitian (2025)

Gambar 1. Algoritma *dHash*

dHash akan menjadi fungsi pembeda dari corak kulit buaya yang digunakan untuk setiap produk. Produk nanti akan diambil gambarnya untuk diperoleh nilai *hash*-nya (*hash value*). Sehingga setiap produk dapat divalidasi keasliannya dengan cara mengambil gambarnya untuk dihasilkan nilai *hash*-nya. Selanjutnya nilai *hash* tersebut akan dibandingkan dengan nilai *hash* dari produsen dengan mempertimbangkan ambang batas *hamming distance* kurang dari sama dengan 10 (≤10) (Bookstein et al., 2002). Jika memiliki *hash value* lebih dari 10 maka produk dikatakan palsu.

4. Skema Anti Pemalsuan Produk Berbahan Kulit Buaya



Sumber : Penelitian (2025)

Gambar 2. Skema anti pemalsuan yang diusulkan

Proses pengolahan produk berbahan kulit buaya terbagi dalam empat tahap:

a. Tahap Pra-Inisialisasi
   1) Pemasok kulit buaya mengemas dan memberikan tanda khusus (stiker) untuk menandai bagian kulit buaya yang akan difoto guna mendapatkan nilai hash (Rogaway & Shrimpton, 2004).
   2) Selanjutnya pemasok harus mengisi informasi detail mengenai kulit buaya, termasuk tujuan produsen penerima agar memperoleh nomor registrasi kulit buaya yang akan dipasok.
   3) Kemudian pemasok mengirimkan foto beserta informasi detail kulit buaya ke *server* asosiasi atau instansi terkait untuk disimpan pada *database*. Data yang tersimpan meliputi: (a) CLR_RG, nomor registrasi yang diberikan oleh asosiasi/instansi; (b) CLR_SN, nomor seri kulit buaya yang dikeluarkan oleh pemasok; (c) CLR_SpN, nama penyedia/pemasok; (d) CLR_PD, tanggal produksi kulit buaya; (e) CLR_PD, nama produsen tujuan; dan (f) CLR_Dt, *detail* tentang kulit buaya seperti lebar, usia buaya saat diproduksi, dan lain-lain. Foto

yang dikirimkan akan dihasilkan *hash value* dari *server* asosiasi dan akan dikorelasikan dengan informasi *detail* kulit buaya yang dikirimkan.

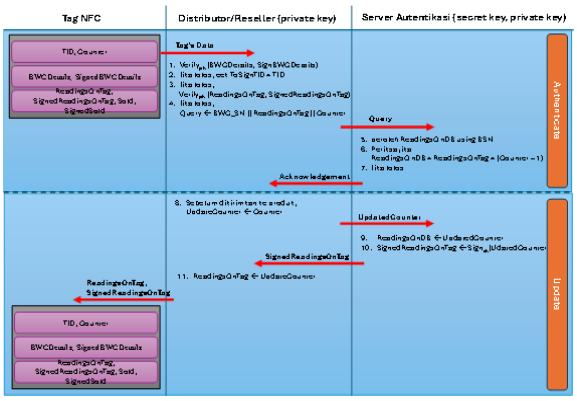
4) Lalu pemasok mengirimkan kulit buaya kepada produsen untuk diolah menjadi produk jadi seperti tas atau dompet.

b. Tahap Inisialisasi

1) Pada saat menerima kulit buaya dari pemasok, produsen harus mengambil foto bagian kulit buaya yang telah diberi stiker untuk menghasilkan *hash value* yang kemudian akan dikirimkan ke *server* asosiasi atau instansi untuk memverifikasi legalitas kulit buaya tersebut. Jika *hash value* sesuai, produsen dapat melanjutkan proses produksi. Sebaliknya, apabila tidak ada *hash value* yang cocok maka kulit buaya tersebut dianggap ilegal dan tidak boleh diproduksi menjadi produk komersial. Asosiasi atau instansi berhak menarik kulit buaya tersebut dari produsen dan meminta klarifikasi kepada pemasok.
2) Setelah produk jadi, tas atau dompet akan dikemas dan dilengkapi tanda khusus (stiker) untuk menunjukkan bagian kulit buaya yang perlu difoto. Ini bertujuan untuk mendapatkan *hash value* yang kemudian akan disimpan dalam *database* produsen sebagai acuan saat membandingkan *hash value* dari gambar yang diambil baik oleh distributor / *re-seller* maupun pelanggan.
3) Selain itu, produk akan dilengkapi dengan *QR Code* untuk meningkatkan keamanan dan kepercayaan terhadap keasliannya. *QR Code* ini akan terbaca oleh distributor / *re-seller* saat produk terjual yang menyebabkan status produk berubah menjadi "*Sold*" atau terjual.
4) Kemudian produsen melakukan data *detail* produk yang mencakup nomor seri produk, warna dan tipe, nama atau inisial produsen, tanggal produksi, dan *hash value* yang diperoleh dari langkah sebelumnya (ToSignBWC) termasuk nilai *Counter* yang digunakan untuk mencatat berapa kali *tag NFC* telah dibaca.

Data yang tersimpan pada *tag NFC* didefinisikan sebagai berikut:

1. BWCDetails ← BWC_SN || BWC_Color&Type || Pd_Name || BWC_Date || ToSignBWC || ToSignTID, dimana: (a) BWCDetails merupakan *detail* produk; (b) BWC_SN merupakan nomor seri produk; (c) BWC_Color&Type merupakan warna dan tipe produk; (d) Pd_Name merupakan nama atau inisial dari produsen; (e) BWC_Date merupakan tanggal produksi; (f) ToSignBWC = nilai *hash* produk; (g) ToSignTID = TID yang merupakan ID tag
2. Signed_BWCDetails = Signedp.sk(BWC_Details), dimana: (a) Signed_BWCDetails merupakan tanda tangan digital *detail* produk; (b) Signedp.sk(BWCDetails) merupakan fungsi tanda tangan digital; (c) p.sk merupakan kunci privat produsen
3. ReadingsOnTag ← Counter, dimana: (a) ReadingsOnTag merupakan nilai pembacaan *tag NFC* saat ini; (b) Counter merupakan nilai pembacaan *tag NFC* yang otomatis akan bertambah setiap kali *tag NFC* dibaca.
4. SignedReadingsOnTag = Signedp.sk(ReadingsOnTag), dimana: (a) SignedReadingsOnTag merupakan tanda tangan digital ReadingsOnTag; (b) Signedp.sk (ReadingsOnTag) merupakan fungsi tanda tangan digital; (c) p.sk merupakan kunci privat produsen
5. "*Sold*" atau terjual merupakan status penjualan produk dengan status awal "Belum Terjual"
6. SignedSold = Signedp.sk(Sold), dimana: (a) SignedSold merupakan tanda tangan digital status penjualan produk; (b) Signedp.sk(Sold) merupakan fungsi tanda tangan digital; (c) p.sk merupakan kunci privat produsen, dengan:
   a. Nilai *hash* dan *QR Code* ini harus dikaitkan dengan data registrasi produk dan selanjutnya disimpan dalam basis data produsen beserta data-data lainnya.
   b. Data registrasi produk juga disimpan dalam *tag NFC* tag pada produk.



Sumber : Penelitian (2025)

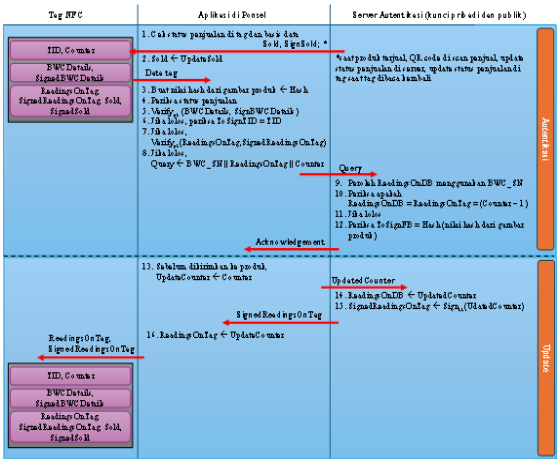
Gambar 3. Proses otentikasi dan perubahan data pada saat produk di rantai pasokan (distributor / *re-seller*)

c. Tahap Otentikasi pada Rantai Pasokan

Setelah produk diterima, distributor / *re-seller* / penjual melakukan otentikasi keaslian produk dengan memindai *tag NFC* yang terdapat pada produk. Proses ini memverifikasi data-data yang terdapat pada *tag NFC* termasuk *Counter* yang otomatis akan bertambah nilainya setiap kali dibaca. Data tersebut akan dikirim secara *online* ke *server* otentikasi produsen untuk membandingkan dengan data yang tersimpan di *database*.
Kemudian, data pada *database* produsen akan diperbarui dan dikirim kembali untuk disimpan pada *tag NFC*. Apabila semua proses tersebut telah selesai, maka produk siap untuk dijual kepada pelanggan.

d. Tahap Otentikasi pada Pelanggan

1) Pada saat produk dibeli (terjual), distributor / *re-seller* / penjual membaca *QR Code* dan langsung meng-*update* data status penjualan di *database* dari "Belum Terjual" menjadi "*Sold*" atau terjual.
2) Pelanggan dapat melakukan otentikasi produk dengan cara (1) mengambil foto produk sesuai tanda khusus (stiker) untuk memperoleh *hash value* dengan algoritma *dHash*; lalu (2) membaca *tag NFC*. Selanjutnya data hasil pembacaan *tag NFC* dan *hash value* dikirim ke *server* otentikasi sebagai pembanding. Data pada *tag NFC* (*detail* dan *counter* produk) akan dibandingkan dengan data yang ada di *database*, jika sesuai proses otentikasi dilanjutkan dengan membandingkan *hash value* dari foto yang diambil pelanggan dengan *hash value* yang tersimpan di *database* produsen. Jika *hash value* memiliki *hamming distance* ≤ 10, maka produk tersebut asli, dimana *hamming distance* adalah ambang batas jumlah perbedaan *hash value* yang dapat ditoleransi. Terakhir lakukan pembaharuan data yang ada di *database* dan mengirimkannya kembali untuk di-*update* pada *tag NFC*, termasuk pembaharuan nilai status penjualan produk "*Sold*" atau terjual.



Sumber : Penelitian (2025)

Gambar 4. Proses otentikasi dan perubahan data pada saat produk sudah dibeli

III. HASIL DAN PEMBAHASAN

Untuk mengetahui bahwa skema anti pemalsuan ini dapat mendeteksi serangan penerapan ulang *tag NFC*, skema akan dievaluasi dengan tiga skenario serangan, yaitu *tag NFC* yang dimodifikasi, dikloning, dan diterapkan kembali (Lehtonen et al., 2008).

1. Serangan Modifikasi *Tag NFC*

Skenario ini dilakukan dengan memodifikasi atau mengubah data yang terdapat pada *tag NFC*. Lalu dengan data yang telah dimodifikasi, pemalsu akan menempelkan *tag NFC* pada produk palsu sehingga produk tersebut tampak seperti produk asli.
Jika pemalsu melakukan skenario serangan tersebut maka *detail* produk (BWCDetails) yang telah ditandatangani secara digital (Signed_BWCDetails) dapat diverifikasi menggunakan kunci privat produsen (p.sk). Sehingga jika ada detail produk yang diubah maka tanda tangan tersebut menjadi tidak valid.

2. *Cloning Attack*

Skenario ini dilakukan pemalsu dengan cara menduplikasi *tag NFC*, sehingga terdapat lebih dari satu *tag NFC* dengan data yang sama seperti pada tag NFC asli. Jika pemalsu "memaksa" melakukan skenario serangan tersebut, maka harus melakukan modifikasi setiap identitas *tag NFC* yang unik. Sebab setiap *tag NFC* yang disematkan pada produk asli memiliki identitas unik yang hanya bisa dibaca (*Tag ID* / *TID*) dan tidak dapat diubah atau ditimpa. Selain itu *TID* ini juga digabungkan ke dalam detail produk (BWCDetails), sebagai ToSignTID. Selanjutnya, dengan menggunakan kunci privat produsen (p.sk), BWCDetails ditandatangani secara digital dan pembacaan *TID* dilibatkan dalam proses verifikasi tanda tangan ini. Untuk lebih jelasnya, perhatikan skenario berikut:

a. Misal *tag NFC* yang disematkan pada produk

asli memiliki TID = T1 dan ToSignTID = T1, menyimpan detail produk BWC1 (BWCDetails).

b. Pemalsu menyalin detail tersebut ke tag lain yang memiliki TID = TX yang nantinya akan disematkan pada produk palsu.
c. Pada saat otentikasi dilakukan, aplikasi verifikasi akan membaca informasi yang tersimpan dalam tag, yaitu identitas tag palsu (TID=TX), *detail* produk (BWCDetails), dan tanda tangan produk (Signed_BWCDetails). Selanjutnya, dengan menggunakan kunci publik produsen (p.pk), aplikasi melakukan verifikasi Signed_BWCDetails yang disediakan oleh BWCDetails. Jika BWCDetails dimodifikasi oleh pemalsu sehingga nilai ToSignTID=TX, maka pada saat proses verifikasi Signed_BWCDetails akan terdeteksi modifikasi tersebut. Namun, jika tidak ada upaya modifikasi BWCDetails oleh pemalsu, maka pada saat verifikasi ToSignTID=TID akan terdeteksi bahwa *tag* tersebut telah dikloning. Hal ini karena aplikasi akan membandingkan ToSignTID=T1 dan TID=TX.

3. Serangan Penerapan Ulang Tag *NFC*

Skenario ini dilakukan dengan cara menggunakan kembali tag *NFC* dari produk asli dan menerapkannya pada produk palsu, sehingga seolah-olah produk palsu tersebut adalah produk asli. Jika pemalsu melakukan skenario serangan tersebut, skema ini dapat menyelesaikannya. Perhatikan skenario berikut:

a. Pemalsu melakukan serangan penerapan ulang *tag NFC* dengan atau tanpa membaca *tag NFC* pada produk akan sulit dideteksi karena skema yang digunakan untuk otentikasi dijalankan secara *online*, sehingga data ReadingsOnTag akan selalu ter-*update* dan sama dengan nilai (Counter-1).
b. Pada tahap inisialisasi *tag NFC* produk (BWC1) akan menyimpan nilai awal yaitu Counter=0, ReadingsOnTag=0, dan ReadingsOnDB=0.
c. Selanjutnya, produk akan didistribusikan melalui rantai pasok dan diotentikasi. Misal produk BWC1 telah sampai di *node* terakhir (*re-seller* atau penjual yang sebelumnya melewati *node* pertama yaitu distributor) yaitu *node* kedua di rantai pasokan. *Re-seller* / penjual ini akan melakukan otentikasi yang mengakibatkan nilai ReadingsOnTag berubah menjadi 2 dimana yaitu:
    1) Nilai awalnya ReadingsOnTag adalah 0
    2) Masuk pada rantai pasokan di *node* pertama (distributor), maka nilai ReadingsOnTag=1

Perubahan nilai ini kemudian dicatat kembali pada ReadingsOnTag, SignedReadingsOnTag, dan kunci publik produsen (p.pk) ke *tag NFC*.

d. Asumsi telah terjadi serangan penerapan ulang *tag* dimana pemalsu memindahkan *tag* produk BWC1 ke produk BWC2 yang merupakan produk palsu (dengan atau tanpa membaca *tag NFC* terlebih dahulu).
e. Selanjutnya, produk palsu BWC2 dibeli oleh pembeli A (korban). Pembeli A lalu melakukan otentikasi produk palsu BWC2 dengan menggunakan telepon genggamnya (Hunegnaw & Bagane, n.d.). Nilai *counter* saat ini adalah 3 karena pada saat otentikasi, *tag* terbaca dan memicu penambahan nilai secara otomatis pada nilai *Counter*. Aplikasi otentikasi pada telepon seluler Pembeli A menjalankan proses otentikasi yang sama dengan yang dilakukan *node* (distributor / *re-seller*) dalam rantai pasokan dan menunjukkan bahwa produk tersebut asli.
f. Pada skema ini, Pembeli A diharuskan mengambil foto produk BWC2 sesuai tanda stiker khusus yang ditempelkan pada bagian produk tersebut untuk memperoleh *hash value* dengan algoritma *dHash*. Setelah *hash* dihasilkan Pembeli A dapat membaca *tag* untuk melakukan otentikasi dengan cara membandingkan nilai *hash* yang baru diperoleh dengan nilai *hash* yang tersimpan dalam *tag* ToSignBWC. Hal ini akan mendeteksi adanya serangan penerapan ulang *tag NFC*.

Selain itu, skema ini juga dapat mendeteksi skenario serangan jika pemalsu mencoba meniru pola produk BWC1, karena:

1. Bagian produk yang harus difoto untuk memperoleh *hash value* diberi tanda/stiker khusus yang diletakkan secara acak. Jika bagian gambar yang diambil berbeda dengan bagian tanda khusus (stiker) pada produk asli, maka akan menghasilkan nilai piksel dan nilai *hash* yang berbeda pula.
2. Produk kulit buaya memiliki corak yang unik yang berbeda dengan corak kulit buaya lainnya sehingga akan mempengaruhi nilai *pixel* citra yang berujung pada perbedaan nilai *hash*.

IV. KESIMPULAN

Skema anti-pemalsuan ini memanfaatkan *tag NFC*, kriptografi kunci publik, dan *dHash* untuk dapat mendeteksi skenario serangan pemalsuan dengan beberapa skenario, yaitu skenario serangan modifikasi *tag NFC*, *cloning attack* dan penerapan ulang *tag NFC*. Selain itu skema ini juga dapat memantau pemanfaatan kulit buaya untuk produk-produk komersial secara legal sehingga membantu dalam menjaga populasi buaya.

Solusi serangan pemalsuan produk adalah adanya asosiasi antara *tag NFC* dengan produknya. Hal ini disediakan melalui pemanfaatan *dHash* untuk mendeteksi kesamaan dua gambar. Pendekatan ini membandingkan *hash* dari gambar produk yang diambil oleh produsen dan oleh distributor / *re-*

seller maupun pembeli.

Keterbatasan dari studi ini adalah adanya kemungkinan kondisi dimana *hash value* yang diperoleh distributor / *re-seller* maupun pembeli secara signifikan berbeda dari *hash value* yang dihasilkan oleh produsen. Dengan kata lain memiliki nilai *hamming distance* > 10, sehingga seolah-olah itu adalah produk palsu. Hal ini dapat dipengaruhi oleh beberapa faktor seperti faktor pencahayaan yang minim atau berlebih pada saat pengambilan gambar produk.

V. REFERENSI

Blankenburg, M., Horn, C., & Krüger, J. (2015). Detection of counterfeit by the usage of product inherent features. *Procedia CIRP*, *26*, 430–435. https://doi.org/10.1016/j.procir.2014.07.062

Bookstein, A., Kulyukin, V. A., & Raita, T. (2002). Generalized hamming distance. *Information Retrieval*, *5*(4), 353–375. https://doi.org/10.1023/A:1020499411651

Bulusu, N., & Alzahrani, N. (n.d.). *Securing Pharmaceutical and High-Value Products Against Tag Reapplication Attacks Using NFC Tags*.

Coskun, V., Ozdenizci, B., & Ok, K. (2013). A survey on near field communication (NFC) technology. In *Wireless Personal Communications* (Vol. 71, Issue 3, pp. 2259–2294). https://doi.org/10.1007/s11277-012-0935-5

Farisa, S., Haviana, C., & Kurniadi, D. (2016). Average Hashing for Perceptual Image Similarity in Mobile Phone Application. *Journal of Telematics and Informatics (JTI)*, *4*(1), 12–18.

Fei, M., Ju, Z., Zhen, X., & Li, J. (2017). Real-time visual tracking based on improved perceptual hashing. *Multimedia Tools and Applications*, *76*(3), 4617–4634. https://doi.org/10.1007/s11042-016-3723-5

Hunegnaw, Y., & Bagane, P. (n.d.). *NFC based Anti-Counterfeiting Scheme for Certificates Identification and Verification using a Smartphone*. http://www.ijpam.eu

Lehtonen, M., Staake, T., Michahelles, F., & Fleisch, E. (2008). From identification to authentication - A review of RFID product authentication techniques. *Networked RFID Systems and Lightweight Cryptography: Raising Barriers to Product Counterfeiting: First Edition*, 169–187. https://doi.org/10.1007/978-3-540-71641-9_9

Lin, W. (2023). Digital signature. In *Trends in Data Protection and Encryption Technologies* (pp. 77–81). Springer Nature. https://doi.org/10.1007/978-3-031-33386-6_15

McKeown, S. (2025). Beyond Hamming Distance: Exploring spatial encoding in perceptual hashes. *Forensic Science International: Digital Investigation*, *52*(S), 301878. https://doi.org/10.1016/j.fsidi.2025.301878

Monga, V., & Evans, B. L. (n.d.). *Perceptual Image Hashing Via Feature Points: Performance Evaluation And Trade-Offs*.

Naumenko, V. (2025). *COMPARATIVE ANALYSIS OF IMAGE HASHING ALGORITHMS FOR VISUAL National Aerospace University " Kharkiv Aviation Institute ", Kharkiv , Ukraine*. *April*. https://doi.org/10.32620/reks.2025.1.09

Prabhu Shankar, B., Rajkumar, N., Viji, C., Dinesh Kumar, K., Saravanakumar, S., & Mohanraj, A. (2024). Approach to Identifying Counterfeit Products with QR Codes and Computational Algorithms. *Proceedings of the 5th International Conference on Smart Electronics and Communication, ICOSEC 2024*, 1203–1209. https://doi.org/10.1109/ICOSEC61587.2024.10722545

Rogaway, P., & Shrimpton, T. (2004). Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 3017, pp. 371–388). https://doi.org/10.1007/978-3-540-25937-4_24

Saeed, M. Q., Bilal, Z., & Walter, C. D. (2013). An NFC based consumer-level counterfeit detection framework. *2013 11th Annual Conference on Privacy, Security and Trust, PST 2013*, 135–142. https://doi.org/10.1109/PST.2013.6596047

Samanta, P., & Jain, S. (2021). Analysis of Perceptual Hashing Algorithms in Image Manipulation Detection. *Procedia Computer Science*, *185*, 203–212. https://doi.org/10.1016/j.procs.2021.05.021

Santos, H. Dos, Martins, T. D. S., Barreto, J. A. D., Nakamura, L. H. V., Ranieri, C. M., De Grande, R. E., Filho, G. P. R., & Meneguette, R. I. (2024). ChaSAM: An Architecture Based on Perceptual Hashing for Image Detection in Computer Forensics. *IEEE Access*, *12*(July), 104611–104628.

https://doi.org/10.1109/ACCESS.2024.3435027

Sutheebanjard, P., & Premchaiswadi, W. (n.d.). *QR-Code Generator*. http://bit.ly/cYEJJe.qr

Tarempa, G. N., & Syalim, A. (n.d.). *dHash-based Anti-Counterfeiting Scheme: Against Tag Re-application Attacks on Batik Tulis*.

Tiwari, S. (2017). *An Introduction to QR Code Technology*. 39–44. https://doi.org/10.1109/icit.2016.021

Warasart, M., & Kuacharoen, P. (n.d.). *Paper-based Document Authentication using Digital Signature and QR Code*.