**Nama : Kadek Vincky Sedana 1808561071**

**I Kadek Aldy Oka Ardita 1808561091**

**Kelompok : 5**

**Mata Kuliah : Kriptoanalisis**

**Review Paper : On the Contrast in Visual Cryptography Schemes\***

1. **introduction**

Skema kriptografi visual (VCS) untuk himpunan P dari n peserta adalah metode untuk menyandikan agambar rahasia SI menjadi n gambar bayangan yang disebut bagian, di mana setiap peserta dalam P menerima satu saham.

Model oleh Naor dan Shamir telah diperluas di [1] dan [2] untuk akses umumstruktur (struktur akses adalah spesifikasi dari semua himpunan bagian yang memenuhi syarat dan terlarang daripeserta), di mana teknik umum untuk membangun VCS untuk setiap struktur akses memilikitelah diusulkan.

Beberapa generalisasi lain dari model dasar telah dipertimbangkan:

• Dalam menerapkan VCS mungkin berguna untuk menyembunyikan keberadaan rahasiapesan, yaitu, bagian yang diberikan kepada peserta dalam skema tidak boleh terlihatseperti sekelompok piksel acak, tetapi mereka harus menjadi gambar yang tampak polos (arumah, anjing, pohon, ...).

• Droste [9] menganggap masalah berbagi lebih dari satu gambar rahasia di antara ahimpunan peserta. Misalnya, dalam Lampiran [9], 2 dari 3 ambang VCSdisajikan di mana setiap pasangan transparansi mengungkapkan gambar rahasia yang berbeda.

• Dalam [16] metode rekonstruksi alternatif untuk VCS dipelajari. Metode ini menghasilkankontras yang lebih tinggi dalam gambar yang direkonstruksi untuk 2 dari n skema ambang batas, tetapiteknik ini tidak berlaku untuk k dari n skema ambang dengan k 3.

• Ukuran kontras alternatif dipertimbangkan dalam [18].

• VCS untuk mengenkripsi gambar berwarna diberikan dalam [13], [17], dan [18].

• Metode otentikasi menggunakan kriptografi visual dipelajari di [14].

1. **Model**

Setiap piksel dari gambar asli akan dikodekan menjadi n piksel, yang masing-masing terdiri dari m subpiksel. Untuk membagikan piksel putih (resp. hitam), dealer secara acak memilih satudari matriks di C 0 (resp. C 1), dan mendistribusikan baris i ke peserta i. Dengan demikian, yang terpilih matrix mendefinisikan m subpiksel di masing-masing n transparansi. Perhatikan bahwa di sebelumnyadefinisi C 0 (resp. C 1) adalah multiset matriks boolean n × m.

Oleh karena itu kami mengizinkan matriks muncul lebih dari sekali di C 0 (resp. C 1). Akhirnya, amati bahwa ukurankoleksi C 0 dan C 1 tidak harus sama. Properti pertama terkait dengan kontras gambar. Ini menyatakan bahwa ketika kualifikasi sekumpulan pengguna menumpuk transparansi mereka, mereka dapat dengan benar memulihkan gambar yang dibagikan olehpedagang. Nilai (m) disebut selisih relatif, bilangan (m) · m disebutsebagai kontras gambar, dan set { t X } X ∈ 0 disebut himpunan ambang batas. Kami ingin kontras menjadi sebesar mungkin dan setidaknya satu, yaitu, (m) 1 /m. Kedua properti disebut keamanan, karena itu menyiratkan bahwa, bahkan dengan memeriksa semua saham mereka, aset peserta terlarang tidak dapat memperoleh informasi apa pun dalam memutuskan apakah yang dibagikanpiksel berwarna putih atau hitam.

Misalkan (Qual , Forb) adalah struktur akses yang kuat dan anggaplah C 0 dan C 1 adalah arekumpulan matriks dalam a ( Qual , Forb , m) -VCS dengan beda relatif (m) . Kemudiankita juga dapat melihat C 0 dan C 1 sebagai VCS untuk struktur akses lemah terkait (0 , Forb ) .Lebih tepatnya, C 0 dan C 1 terdiri dari ( 0 , Forb , m) -VCS dengan perbedaan relatif padapaling sedikit (m) .Ada beberapa perbedaan antara model kriptografi visual yang kami usulkan danyang disajikan oleh Naor dan Shamir [15]. Model kami adalah generalisasi dari yang satudiusulkan dalam [15], karena dengan setiap set X ∈ Qual kita kaitkan (mungkin) berbedaambang t X.

Selanjutnya, struktur akses tidak harus kuat dalam model kami. Perhatikan bahwa jika himpunan peserta X adalah superset dari himpunan X yang memenuhi syarat , maka mereka dapatmemulihkan gambar bersama dengan mempertimbangkan hanya bagian dari set X . Ini tidak masuksendiri mengesampingkan kemungkinan bahwa menumpuk semua transparansi peserta di Xtidak mengungkapkan informasi apa pun tentang gambar yang dibagikan.Kami membuat beberapa pengamatan tentang struktur Qual dan Forb sehubungan dengandefinisi di atas. Pertama, jelas bahwa setiap subset dari subset terlarang dilarang, jadi

1. **Skema ambang batas**

Dalam makalah ini kami menyajikan teknik baru untuk mewujudkan (k, n) -ambang pencapaian VCSnilai yang lebih besar dari perbedaan relatif ketika k < n . Dalam kasus ( 2 , n) -ambangVCS, kami memperoleh nilai terbaik untuk perbedaan relatif (lihat Teorema 4.2), sebagai,memberikan karakterisasi lengkap dari skema yang mencapai kemungkinan relatif terbesarperbedaan dan perluasan piksel seminimal mungkin. Dalam [5] bentuk kanonik untuk (k, n) -ambang VCS disajikan dan lengkapkarakterisasi kontras optimal (n 1 , n) -ambang VCS dalam bentuk kanonik adalahdiberikan. Selain itu, untuk n 4, kontras optimal ( 3 , n) -ambang VCS dalam bentuk kanoniktelah di sediakan. Akhirnya, untuk k = 4 , 5 dua skema dengan kontras asimtotik sama1 / 64 dan 1 / 256, masing-masing, disajikan.

1. **( 2 , n ) -VCS Ambang dengan Kontras Optimal**

Di bagian ini kami menjelaskan ( 2 , n) -ambang VCS mencapai perbedaan relatif yang lebih besardaripada yang disajikan dalam [1], [2], [9], dan [15]. (Konstruksi ini pertama kali disebutkandalam [2] dan konstruksi serupa dalam kasus di mana n genap diberikan dalam Bagian 5.2dari [10].)

**5. Konstruksi untuk a ( k , n ) -Threshold VCS**

Pada bagian ini penulis memberikan beberapa konstruksi baru untuk (k, n) -threshold VCS yang memiliki tinggi perbedaan relatif (m). Untuk membangun skema ini, dibutuhkan matriks awal yang telah didefinisikan sedemikian rupa.

**6. Struktur a ( k , n ) -Threshold VCS**

Di bagian ini penulis memberikan kondisi yang diperlukan dan cukup untuk keberadaan yang lemah (k, n) -threshold VCS yang direalisasikan menggunakan matriks basis. Hal ini memungkinkan kita untuk membuktikan lebih rendah keterikatannya pada ekspansi piksel dan batas atas pada perbedaan relatif. Kedua batas juga berlaku untuk kasus a (k, n) -threshold VCS. Akhirnya, penulis dapat menunjukkan bagaimana hasil di perbedaan relatif dapat diperluas ke kasus umum skema yang direalisasikan menggunakan koleksi matriks Boolean.

**7. Struktur Matriks Basis**

Pada bagian ini penulis menganalisis struktur matriks basis dan dari (k, k) -threshold VCS. Penulis mengatakan bahwa kolom atau genap (ganjil) jika memiliki nomor genap (ganjil) entri sama dengan 1.