Skema *Fragile Watermarking* dengan Fungsi *Hash* dan Ketergantungan Blok Tak Deterministik

Rubiano Adityas[#1], Dr. Ir. Rinaldi Munir, M. T.#[2]

[#]*Departemen Teknik Informatika, Institut Teknologi Bandung*
Jalan Ganesha 10 Bandung 40132, Indonesia
[1]13510041@std.stei.itb.ac.id
[2]rinaldi@informatika.org

Abstrak— ***Digital watermarking* merupakan sebuah metode untuk menyisipkan sebuah media *watermark* ke dalam media yang ingin dilindungi, dan mengekstraksi kembali media *watermark* untuk kemudian dianalisis sesuai tujuan implementasinya. Secara umum digital *watermark* ada dua tipe, yaitu *robust watermarking* untuk perlindungan hak cipta, dan *fragile watermarking* untuk otentikasi pemilik. Salah satu skema yang sudah dikembangkan untuk *fragile watermarking* adalah skema ajuan Wong. Skema Wong mampu mendeteksi serangan-serangan sederhana seperti geometri dan *forgery*, namun tidak bisa mendeteksi serangan Holliman-Memon dan transplantasi.**

Skema-skema lain sudah dikembangkan untuk menangani serangan Holliman-Memon dan transplantasi, seperti Skema Wu dkk. dan Yuan dkk.. Skema *fragile watermarking* dengan ketergantungan blok terbukti mampu mendeteksi serangan Holliman-Memon, sementara ketergantungan blok tak deterministik mampu mendeteksi serangan transplantasi. Dilakukan modifikasi terhadap Skema Wong dengan penambahan aspek-aspek dari Skema Wu dkk. dan Skema Yuan dkk., agar skema modifikasi memiliki ketergantungan blok tak deterministik.

Dari hasil pengujian, diketahui bahwa skema modifikasi Wong mampu mendeteksi serangan *forgery*, geometri, Holliman-Memon, dan transplantasi, sebagaimana skema-skema ketergantungan blok tak deterministik lainnya.

Keywords— ***fragile watermarking*, Skema Wong, serangan Holliman-Memon, serangan transplantasi, ketergantungan blok tak deterministik.**

I. PENDAHULUAN

Seiring dengan perkembangan infrastruktur dan popularitas teknologi internet, publikasi dan distribusi media digital semakin mudah untuk dilakukan. Beragam bentuk media digital, seperti video dan citra, dapat diakses dengan mudah oleh pengguna komputer yang terhubung dengan jaringan internet. Kemudahan publikasi dan distribusi media digital ini dapat dimanfaatkan untuk e-commerce, tujuan akademik, maupun sekedar berbagi pengalaman dan hiburan dengan teman. Meski kemudahan akses terhadap media digital memberikan beragam keuntungan, hal ini dapat dimanfaatkan oleh pihak yang tidak bertanggungjawab untuk memanipulasi media untuk tujuan yang tidak seharusnya. Untuk menangani hal tersebut, dikembangkan sebuah metode untuk melindungi dan mengotentikasi media digital, yaitu digital *watermarking*.

Digital *watermarking* adalah proses penyisipan *watermark* kedalam sebuah media digital, dimana *watermark* yang disisipkan nantinya dapat diekstrak kembali untuk berbagai macam tujuan. Berbagai macam metode *watermarking* sudah dikembangkan demi memenuhi berbagai macam tujuan yang berbeda, namun secara umum dapat dibagi menjadi dua tipe, yaitu *robust watermarking* dan *fragile watermarking*. *Robust watermarking* biasa digunakan untuk melindungi hak cipta sebuah media digital, sementara *fragile watermarking* digunakan untuk otentikasi pemilik media digital[5].

Salah satu metode *fragile watermarking* citra adalah skema yang diajukan oleh Wong[14], yang berbasiskan partisi blok citra dan menggunakan fungsi *hash* MD5. Metode tersebut mampu melokalisasi perubahan dengan baik. Skema Wong tidak memiliki ketergantungan blok, dan hal tersebut menjadi celah untuk serangan Holliman-Memon[5]. Untuk mengatasi hal tersebut, sudah diajukan beberapa solusi berupa implementasi ketergantungan blok pada Skema Wong, seperti Hash Block Chaining[1] dan skema yang diajukan oleh Wu dkk.[16]. Namun Barreto dkk.[1] telah menunjukkan bahwa skema *fragile watermarking* dengan ketergantungan blok, baik itu Skema Wong yang telah dimodifikasi atau skema lainnya, masih rentan terhadap serangan transplantasi.

Serangan transplantasi memanfaatkan pengetahuan mengenai pola ketergantungan yang digunakan oleh skema ketergantungan blok. Dengan mengetahui blok tetangga mana saja yang digunakan oleh proses penyisipan nilai suatu blok, penyerang dapat menukar sekumpulan blok yang memiliki ketergantungan yang sama sehingga skema tidak bisa mendeteksi adanya manipulasi.

Agar skema *fragile watermarking* mampu mendeteksi serangan transplantasi, diperlukan skema dengan ketergantungan blok tak deterministik. Salah satu skema yang telah dikembangkan adalah skema ajuan Yuan dkk.[18]. Skema ajuan Yuan dkk. terbukti mampu mendeteksi serangan transplantasi. Makalah ini membahas proses modifikasi Skema Wong dengan aspek ketergantungan blok tak deterministik agar tahan terhadap serangan Holliman-Memon dan transplantasi.

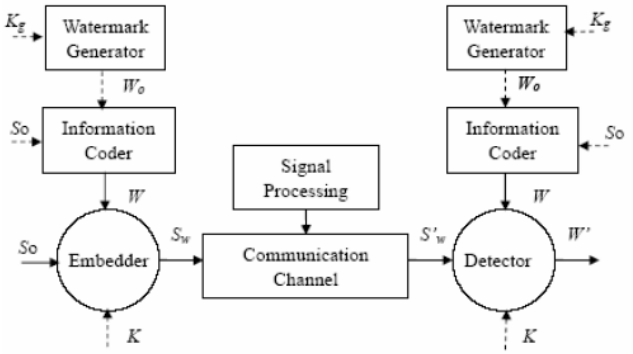
II. LANDASAN TEORI

Dalam landasan teori dibahas beberapa teori yang dipakai dalam makalah ini, yaitu tentang *digital watermarking*, Skema-skema *fragile watermarking* yang relevan, dan

beberapa bentuk serangan terhadap skema *fragile watermarking,* yaitu serangan Holliman-Memon dan transplantasi..

A. *Watermark Digital*

Watermark digital adalah sebuah sinyal digital yang disisipkan ke dalam sebuah dokumen digital, seperti teks, grafik, dan presentasi multimedia[2]. Sebagai teknologi yang relatif baru berkembang, *watermark* digital melibatkan ide dan teori dari beberapa bidang lain, seperti pemrosesan sinyal, kriptografi, teori peluang dan stokastik[13].

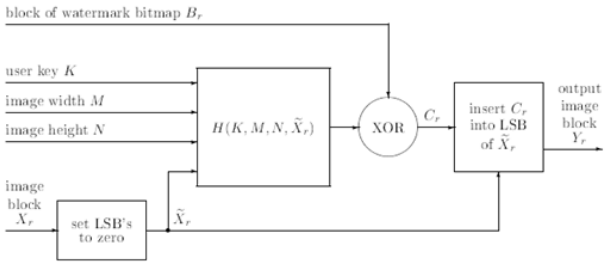


Gambar. 1 Skema Sistem *Watermarking* Umum[3]

Dalam sebuah skema *watermarking*, sebuah media yang akan dikirimkan kepada pihak lain terlebih dulu disisipkan *watermark* dengan menggunakan *embedder*. Keluaran *embedder* adalah citra yang telah tersisipi *watermark*. Citra tersebut kemudian akan dikirimkan melalui sebuah kanal komunikasi, dimana berbagai macam pemrosesan seperti serangan dan kompresi bisa terjadi. Citra yang telah sampai tujuan kemudian dimasukkan ke dalam *detector.* Bagaimana kondisi *watermark* yang terekstraksi apabila terjadi modifikasi pada media original tergantung dari tipe skema *watermarking* yang digunakan. Pada *robust watermarking* yang biasa digunakan untuk perlindungan hak cipta, citra *watermark* diharapkan tidak rusak akibat adanya modifikasi. Namun pada *fragile watermarking* yang biasa digunakan untuk otentikasi kepemilikan, *watermark* diharapkan mengalami kerusakan akibat adanya modifikasi pada media original. Hal tersebut bertujuan untuk mendeteksi ada atau tidaknya modifikasi pada media.

B. *Skema Wong*

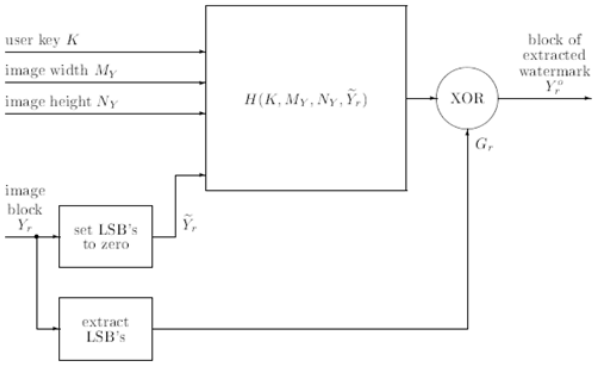
Ping Wah Wong[14] merumuskan sebuah skema *fragile watermarking* untuk media citra yang berbasiskan blok-blok *pixel* dan fungsi *hash*. Skema ini dapat mendeteksi perubahan pada citra secara lokal. Sebuah citra dan *watermark* yang akan disisipkan pada citra terlebih dulu dipartisi menjadi beberapa blok dengan ukuran yang sama. Tiap-tiap blok *watermark* kemudian disisipkan ke dalam blok citra pada posisi koordinat yang sama, dengan metode yang diilustrasikan pada Gambar 2.



Gambar. 2 Diagram Blok Penyisipan Wong[14]

Fungsi *hash* akan menerima kunci pemilik citra, nilai dimensi citra asli, dan blok citra yang nilai LSB dari seluruh *pixel* penyusunnya sudah diganti dengan 0. Penggantian nilai LSB dilakukan agar penghitungan fungsi *hash* tidak menggunakan nilai *pixel* yang nantinya akan digunakan sebagai penyimpan hasil pengolahan *watermark*. Hal ini dilakukan untuk menjaga agar proses penyisipan dan ekstraksi reversibel.

Keluaran fungsi *hash* kemudian digabungkan dengan blok *watermark* menggunakan operasi *exclusive-or* (XOR). Hasil operasi tersebut kemudian dimasukkan ke dalam LSB dari blok citra. Proses diulang terus-menerus hingga seluruh blok citra tersisipi oleh blok *watermark*.



Gambar. 3 Diagram Blok Ekstraksi Wong[14]

Metode ekstraksi *watermark* Skema Wong diilustrasikan pada Gambar 3. Citra ber-*watermark* dipartisi menjadi blok-blok dengan ukuran yang sama dengan ukuran blok ketika proses penyisipan. Tiap-tiap blok partisi diambil seluruh nilai LSB-nya, yang terlebih dulu disimpan. Setelah itu, seluruh *pixel* penyusun blok partisi diubah nilai LSB-nya menjadi 0. Fungsi *hash* menerima blok partisi tanpa LSB, kunci pemilik citra, dan dimensi citra asli sebagai masukan.

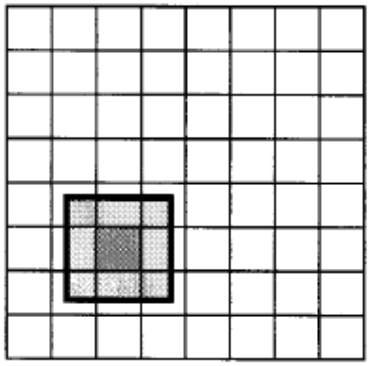
Nilai keluaran fungsi *hash* kemudian digabungkan dengan nilai LSB blok yang sebelumnya disimpan, menggunakan operasi XOR. Proses dilakukan hingga seluruh blok *watermark* terekstraksi, untuk kemudian digabungkan menjadi citra *watermark*.

Dari citra *watermark* yang diekstraksi, dapat dideteksi ada atau tidaknya perubahan. Blok tempat dilakukannya modifikasi akan tampak sebagai derau pada *watermark* yang diekstraksi. Pengujian terhadap performansi Skema Wong ditunjukkan pada Gambar 4. Ilustrasi pada baris pertama adalah citra asli beserta citra *watermark* yang disisipkan ke dalamnya, sementara pada baris di bawahnya adalah citra yang dimodifikasi beserta citra *watermark* yang diekstraksi dari citra tersebut.

Gambar. 4 Pengujian Skema *Watermarking*[14]

C. Skema Wu dkk.

Salah satu modifikasi terhadap Skema Wong adalah Skema Wu dkk.[16]. Modifikasi tersebut adalah implementasi ketergantungan blok ke dalam Skema Wong yang pada mulanya tidak memiliki ketergantungan blok. Komputasi nilai *hash* pada Skema Wong yang sebelumnya hanya menggunakan nilai *pixel* satu blok, dimodifikasi sehingga menggunakan blok-blok di sekitarnya juga.



Gambar. 5 Skema Ketergantungan Blok[16]

Pada Gambar 5, kotak berwarna putih merepresentasikan blok-blok partisi, dan kotak berwarna abu-abu tua merepresentasikan blok citra yang sedang diproses. Sebagai masukan fungsi *hash*, skema menggunakan nilai *pixel* blok citra yang sedang diproses beserta sejumlah *pixel* tetangganya. Kotak dengan batasan hitam tebal merupakan lingkup *pixel-pixel* tetangga yang nilai *pixel*-nya digunakan sebagai masukan fungsi *hash*. Modifikasi ini terbukti membuat skema tahan terhadap seranga Holliman-Memon.

D. Skema Yuan dkk.

Yuan dkk.[18] mengajukan sebuah skema *fragile watermarking* dengan ketergantungan blok tak deterministik. Skema tersebut menggunakan nilai *pixel* penyusun citra *watermark* yang dibangkitkan dengan generator dan kunci sebagai informasi non kontekstual. Informasi non kontekstual tersebut digunakan untuk menentukan tetangga blok mana yang digunakan untuk membentuk *signature* sebuah blok citra. Skema ajuan Yuan terbukti mampu mendeteksi serangan transplantasi.

E. Serangan Holliman-Memon

Holliman dan Memon[5] merumuskan sebuah metode serangan terhadap skema *fragile watermarking* yang tidak memiliki ketergantungan blok. Misal ada sebuah blok citra X yang tersisipi blok *watermark* W, maka serangan Holliman-Memon akan mengganti blok X dengan sebuah blok lain, misal blok Y, yang juga tersisipi blok *watermark* W yang sama. Skema yang tidak memiliki ketergantungan blok seperti Skema Wong tidak akan mendeteksi adanya modifikasi, karena blok *watermark* yang terekstraksi pada posisi blok X akan terlihat identik dengan blok *watermark* W, meski blok X sudah digantikan dengan blok Y.

F. Serangan Transplantasi

Barreto dkk.[1] merumuskan sebuah metode serangan terhadap skema *fragile watermarking* dengan ketergantungan blok yang deterministik. Pada dasarnya metode yang digunakan mirip dengan serangan Holliman-Memon, namun serangan ini juga mempertimbangkan ketergantungan blok ketika ingin mengganti sekumpulan blok citra dengan sekumpulan blok citra lain yang tersisipi di dalamnya sekumpulan blok *watermark* yang identik. Misal ada sekumpulan blok sebagai berikut,

$$\ldots \leftrightarrow X'_A \leftrightarrow X'_B \leftrightarrow X'_E \leftrightarrow X'_C \leftrightarrow X'_D \leftrightarrow \ldots ,$$
$$\ldots \leftrightarrow X''_A \leftrightarrow X''_B \leftrightarrow X''_F \leftrightarrow X''_C \leftrightarrow X''_D \leftrightarrow \ldots ,$$

X'_A identik dengan X''_A, dan seterusnya hingga X'_D dan X''_D, terkecuali blok X'_E dan X''_F. Dua kumpulan blok tersebut juga memiliki blok-blok *watermark* yang sama yang tersisip di dalamnya. Penyerang ingin mengganti X''_F dengan X'_E, maka dari itu penyerang memindahkan X'_E dan blok-blok yang tergantung terhadapnya ke posisi X''_F pada kumpulan blok yang kedua menjadi seperti berikut,

$$\ldots \leftrightarrow X'_A \leftrightarrow X'_B \leftrightarrow X'_E \leftrightarrow X'_C \leftrightarrow X'_D \leftrightarrow \ldots ,$$
$$\ldots \leftrightarrow X''_A \leftrightarrow X'_B \leftrightarrow X'_E \leftrightarrow X'_C \leftrightarrow X''_D \leftrightarrow \ldots ,$$

Modifikasi tersebut tidak mampu dideteksi oleh skema *fragile watermarking* dengan ketergantungan blok yang deterministik.

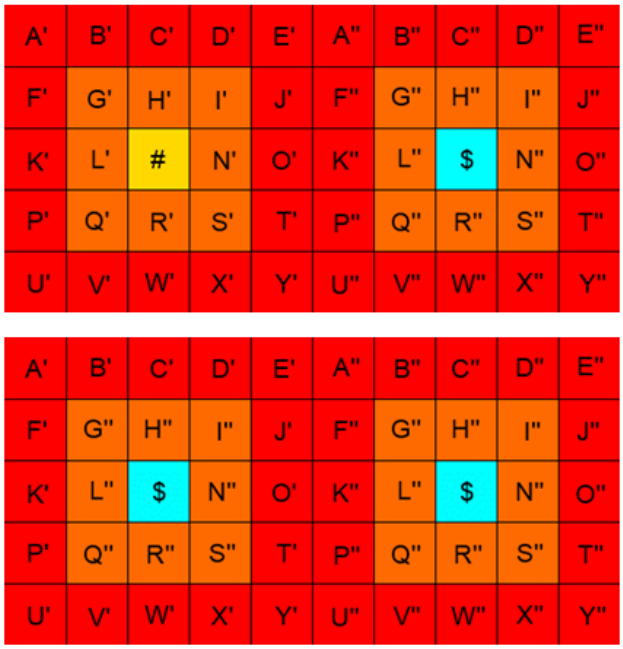
III. ANALISIS SKEMA DASAR

Skema Wong tidak mampu mendeteksi serangan Holliman-Memon, seperti yang ditunjukkan pada Gambar 6. Untuk menangani hal tersebut, Skema Wong dimodifikasi agar memiliki ketergantungan blok. Salah satu modifikasi tersebut adalah Skema Wu dkk.. Skema Wu dkk. terbukti mampu mendeteksi serangan Holliman-Memon seperti yang ditunjukkan pada Gambar 7. Namun, Skema Wu dkk. belum mampu mendeteksi serangan transplantasi. Serangan transplantasi diilustrasikan pada Gambar 9, sementara Gambar 8 merupakan *watermark* original yang disisipkan, yang identik dengan hasil ekstraksi *watermark* setelah serangan dilakukan.

Gambar. 6 Serangan HM Terhadap Skema Wong, Beserta Hasil Ekstraksi

Gambar. 7 Serangan HM Terhadap Skema Wu dkk., Beserta Hasil Ekstraksi

Gambar. 8 *Watermark* Penyisipan dan Hasil Ekstraksi Serangan Transplantasi Terhadap Skema Wu dkk.



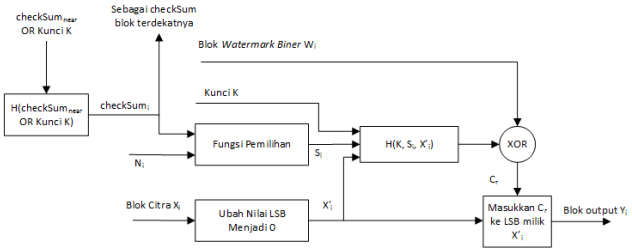
Gambar. 9 Serangan Transplantasi Terhadap Skema Wu dkk

Skema Yuan dkk. merupakan skema *fragile watermarking* dengan ketergantungan blok tak deterministik. Skema *fragile watermarking* dengan ketergantungan blok tak deterministik sudah terbukti mampu mendeteksi serangan Holliman-Memon dan transplantasi. Kekurangan Skema Yuan adalah pengguna tidak bisa memilih citra *watermark* yang ingin disisipkan, karena citra *watermark* bersifat rahasia dan dibangkitkan dengan sebuah generator dan kunci. Pengguna tidak bisa menggunakan citra *watermark* pengenal identitas yang umum seperti logo organisasi atau tanda tangan, sehingga fungsi otentikasi kepemilikan menjadi kurang baik.

Skema Wong dapat menggunakan citra *watermark* berupa logo organisasi atau tanda tangan, sehingga dapat mengotentikasi kepemilikan citra dengan baik. Meski begitu, tingkat keamanannya belum sebanding dengan Skema Yuan. Dengan mengadaptasi fungsi pemilihan tetangga milik Skema Yuan, diharapkan modifikasi Skema Wong mampu tahan terhadap serangan transplantasi, selagi memiliki fungsi otentikasi kepemilikan yang baik.

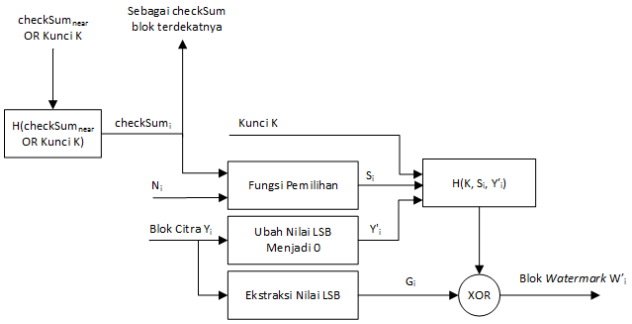
IV. SKEMA YANG DIUSULKAN

Dirancang sebuah modifikasi terhadap Skema Wong, dengan penggunaan beberapa lapis *pixel* tetangga blok seperti skema Wu dkk.. Selain itu, digunakan juga nilai non kontekstual yang tidak diambil dari informasi citra, dan unik untuk setiap blok, yang digunakan untuk memilih tetangga mana yang digunakan dalam penghitungan *signature*. Metode tersebut diadaptasi dari Skema Yuan dkk. yang menggunakan nilai *pixel* dari citra *watermark* sebagai penentu tetangga.



Gambar. 10 Diagram Blok Penyisipan Skema Modifikasi

Alur proses penyisipan *watermark* mirip dengan Skema Wong, seperti yang ditunjukkan pada Gambar 10. Skema tersebut akan menerima partisi blok citra X_i, dan nantinya seluruh blok hasil pemrosesan akan digabungkan kembali. Modifikasi terletak pada fungsi *hash* pembentuk *signature* blok, dimana terjadi pengurangan dua buah masukan, yaitu panjang dan lebar citra. Tujuan awal dari masukan panjang dan lebar citra pada Skema Wong adalah agar skema mampu mendeteksi serangan pemotongan pada ujung citra. Ketergantungan blok tetangga pada skema memberikan fungsionalitas yang sama, maka dari itu kedua masukan tersebut dihilangkan. Selain itu, ada masukan tambahan fungsi *hash* pembentuk *signature* blok berupa nilai keluaran dari fungsi pemilihan. Fungsi pemilihan inilah yang menjadikan skema memiliki ketergantungan blok tak deterministik. Modifikasi yang serupa juga dilakukan untuk proses ekstraksi, seperti yang ditunjukkan pada Gambar 11.



Gambar. 11 Diagram Blok Penyisipan Skema Modifikasi

Fungsi pemilihan akan menerima dua masukan berupa *checksum* dan ketetanggan blok X_i, yaitu N_i. Himpunan N_i pada skema ini beranggotakan *pixel-pixel* yang mengelilingi blok X_i. Jumlah barisan *pixel* ketetanggaan yang termasuk dalam N_i adalah setengah dari panjang sisi blok yang dibulatkan ke bawah. Bila blok *Xi* memiliki panjang sisi 8 *pixel*, maka N_i akan meliputi 4 baris *pixel* yang mengelilingi X_i.

Untuk membuat skema ini menjadi skema dengan ketergantungan blok tak deterministik, dibutuhkan informasi kontekstual dan non kontekstual[8]. Informasi kontekstual didapat dari blok ketetanggaan N_i, sementara informasi non kontekstual didapat dengan menggunakan nilai *hash* dari kunci *K*, yang menjadi *checksum* untuk blok pertama. *checksum* untuk blok paling kiri pada tiap baris blok (kecuali blok pertama) adalah nilai *hash* dari *checksum* blok di atasnya yang dikonkat dengan kunci *K*. Sementara itu, *checksum* untuk blok-blok lain adalah nilai *hash* dari *checksum* blok sebelah kirinya. Aturan tersebut dibuat agar menjamin keunikan informasi non kontekstual untuk tiap blok X_i.

Informasi non kontekstual pada tiap blok tidak langsung digunakan untuk membentuk *signature* blok, melainkan digunakan oleh fungsi pemilihan untuk menentukan *pixel* mana saja pada himpunan N_i yang dilibatkan dalam pembentukan nilai rahasia S_i, yang merupakan salah satu komponen untuk membuat *signature*. Nilai S_i dihitung dengan menggunakan rumus

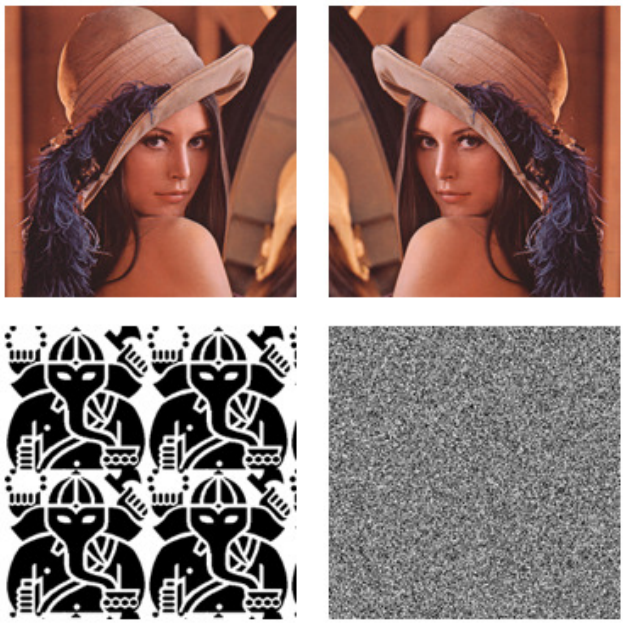
$$S_i = \sum_{j \in N_i} (checkSum_i\,[iterator])\ MSB(j).$$

checksum direpresentasikan dalam bentuk larik biner, dan diakses dengan menggunakan iterator. Dimulai dari nol, nilai iterator bertambah satu ketika memproses anggota N_i berikutnya (nilai *j* bertambah), dan kembali ke nol ketika sudah mencapai panjang maksimal *checksum*. Apabila nilai yang didapat dari *checksum* dengan iterator adalah 1, maka *pixel j* digunakan untuk menghitung nilai S_i. Fungsi MSB(j) memberikan nilai 7 MSB dari *pixel* j.

Keunikan nilai *checksum* untuk tiap blok X_i berperan penting untuk mencegah serangan transplantasi. Apabila ada penyerang yang ingin menyalin sekumpulan blok ke sekumpulan blok lain, skema akan mendeteksi serangan transplantasi tersebut. *checksum* yang merupakan informasi non kontekstual memiliki nilai unik yang tak bergantung konten blok dan blok-blok tetangganya. Meski seluruh blok tetangga dan blok tetangga dari tetangganya identik, dan blok *watermark* yang tersisipi juga identik, *pixel-pixel* blok tetangga yang digunakan akan berbeda, karena tiap blok memiliki *checksum* yang berbeda. Perbedaan tetangga yang digunakan akan menimbulkan derau pada blok X_i ketika proses ekstraksi, sehingga serangan transplantasi terdeteksi.

V. EKSPERIMEN

Hasil eksperimen menunjukkan skema modifikasi mampu mendeteksi semua variasi serangan yang diujikan pada skema Wong dan Wu dkk., yaitu serangan geometri, *forgery*, Holliman-Memon, dan transplantasi. Gambar 12 menunjukkan hasil deteksi serangan geometri, sementara Gambar 13 menunjukkan hasil deteksi serangan *forgery*. Gambar 14 menunjukkan hasil deteksi serangan Holliman-Memon, dan Gambar 15 merupakan hasil ekstraksi *watermark* citra yang diserang dengan metode transplantasi, menggunakan citra yang sama dengan Gambar 9.



Gambar. 12 Serangan Geometri Terhadap Skema Modifikasi

Gambar. 13 Serangan *Forgery* Terhadap Skema Modifikasi

Gambar. 14 Serangan HM Terhadap Skema Modifikasi

Gambar. 15 Hasil Ekstraksi Serangan Transplantasi Terhadap Skema Modifikasi

VI. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, dapat digunakan aspek ketergantungan blok dari Skema Wu dkk. dan aspek tak deterministik dari Skema Yuan dkk., untuk membuat sebuah modifikasi Skema Wong dengan ketergantungan blok tak deterministik yang tahan terhadap serangan Holliman-Memon dan transplantasi. Aspek ketergantungan blok diperoleh dengan penggunaan konten blok-blok tetangga dengan jarak tertentu untuk mengkalkulasi nilai *signature* suatu blok, seperti yang dilakukan oleh Skema Wu dkk.. Aspek tak deterministik diperoleh dengan penggunaan informasi non kontekstual sebagai penentu tetangga mana yang digunakan untuk mengkalkulasi nilai *signature* suatu blok, seperti yang dilakukan oleh Skema Yuan dkk.

Skema modifikasi memiliki properti keamanan yang lebih baik ketimbang skema-skema dasarnya. Hal tersebut dikarenakan skema-skema dasarnya tidak mampu mendeteksi beberapa serangan, seperti Holliman-Memon dan transplantasi, yang mampu dideteksi dengan skema modifikasi. Secara keseluruhan, skema modifikasi mampu mendeteksi serangan forgery, *geometri*, Holliman-Memon, dan transplantasi, sebagaimana skema-skema ketergantungan blok tak deterministik lainnya.

REFERENSI

[1] Barreto, P.S.L.M, dkk. (2002). Towards a Secure Public-Key Blockwise Fragile Authentication Watermarking. Prosiding IEEE – Vision, Image and Signal Processing, 148(2), 57-62.

[2] Berghel, H. (1997). *Watermarking Cyberspace*. Communications of the ACM, vol. 40, no. 11, 19-24.

[3] El-Gayyar, M. (2006). *Watermarking Techniques, Spatial Domain, Digital Rights Seminar*. University of Bronn Germany: Media Informatics.

[4] Fulton, W. (1997). *Image File Formats – JPG, TIF, PNG, GIF, Which to Use?*. http://www.scantips.com/basics09.html. Terakhir diakses tanggal 2 Februari 2014.

[5] Holliman, M., & Memon, N. (2000). *Counterfeiting Attacks on Oblivious Block-wise Independent Invisible Watermarking Schemes*. IEEE Trans. Image Processing, vol. 9, no. 3, 432-441.

[6] Kim, Dae-Hong, dkk. (2010). *Comparison and Evaluation of JPEG and JPEG2000 in Medical Images for CR (Computed Radiography)*. Journal of the Korean Physical Society, vol. 56, no. 3, 856-862.

[7] Li, C.T., & Yang, F.M. (2003). *One-dimensional Neighborhood Forming Strategy for Fragile Watermarking.* Journal of Electric Imaging, vol. 12, no. 2, 284-291.

[8] Menezes, A.J., dkk. (1997). *Handbook of Applied Cryptography*. CRC Press.

[9] National Instruments (2013). *Peak Signal-to-Noise Ratio as an Image Quality Metric*. http://www.ni.com/white-paper/13306/en/. Terakhir diakses tanggal 19 Januari 2014.

[10] Podilchuk, C., & Delp, E. (2001). *Digital Watermarking Algorithms and Applications.* IEEE Signal Processing Magazine, vol. 18, no. 4.

[11] Rivest, R.L. (1992). *The MD5 Message Digest Algorithm*. Internet RPC 1321.

[12] Sachs, J. (1996). *Digital Image Basics*. Digital Light & Color

[13] Singh, P., & Chadha, R.S. (2013). *A Survey of Digital Watermarking Techniques, Applications and Attacks*. International Journal of Engineering and Innovative Technology, vol. 2, issue 9, 165-175.

[14] Wong, P.W. (1997). A Watermark for Image Integrity and Ownership Verification. Prosiding IS&T PIC Conference.

[15] Wong, P.W., & Memon, N.D (2000). Secret and Public Key Authentication Watermarking Schemes that Resist Vector Quantization Attack. Prosiding SPIE Security Watermarking Multimedia Contents II.

[16] Wu, C.W, dkk. (1999). Fragile Imperceptible Digital Watermark with Privacy Control. Prosiding SPIE Security Watermarking Multimedia Contents, vol. 3657.

[17] Yeung, M.M., & Mintzer, F. (1997). An Invisible Watermarking Technique For Image Verification. Prosiding International Conference Image Processing, vol. 1, 680-683.

[18] Yuan, Y., & Li, C.T. (2004). Fragile Watermarking Scheme Exploiting Non-deterministic Block-wise Dependency. Prosiding IAPR International Conference on Pattern Recognition, vol. 4, 849-852. Cambridge, UK.