Skema Proteksi Hak Cipta untuk Citra Warna Digital Menggunakan *Visual Cryptography*

Septia Rani[1], Agus Harjoko[2]

***Abstract*— Currently, cases of misuse of intellectual property such as digital image have occurred frequently. Copyright protection needs to be done to reduce the occurrence of cases of misuse of a digital image by an unauthorized person. Watermark image can be used to mark the ownership of a digital image. In this paper, a copyright protection scheme based on visual cryptography for digital color image is proposed. Visual cryptography is chosen because it is easy to implement and has a high level of security. Unlike most conventional watermarking schemes, the image to be protected is not directly modified by embedding the watermark into it. Visual cryptography technique is used to generate two share images, namely ownership share image and master share image. To identify the ownership of the image, the watermark can be obtained by stacking the master share image with the ownership share image. Some experiments are carried out to assess the robustness and security performance of the proposed scheme. The results show that the proposed scheme meets the security criteria and has shown robustness against image processing attacks, demonstrated by the acquisition of the average value of the extracted watermark accuracy ratio that is equal to 0.94537.**

***Intisari*— Saat ini, kasus penyalahgunaan properti intelektual seperti citra digital sudah banyak terjadi. Perlu dilakukan proteksi hak cipta untuk mengurangi terjadinya kasus penyalahgunaan citra digital oleh orang yang tidak berhak. Untuk menandai kepemilikan terhadap citra digital, dapat digunakan sebuah citra yang disebut *watermark*. Pada makalah ini dikembangkan sebuah skema proteksi hak cipta berbasis *visual cryptography* untuk citra warna digital. Teknik *visual cryptography* dipilih karena mudah diimplementasikan dan memiliki tingkat keamanan yang tinggi. Berbeda dengan kebanyakan skema *watermarking* yang sudah ada, citra yang akan diproteksi tidak dimodifikasi secara langsung dengan menambahkan *watermark*. Skema yang diajukan menggunakan teknik *visual cryptography* untuk membentuk dua buah citra *share*, yaitu citra *ownership share* dan citra *master share*. Untuk melakukan identifikasi kepemilikan citra, *watermark* dapat diperoleh dengan melakukan *stacking* antara citra *master share* dan citra *ownership share*. Beberapa pengujian dilakukan untuk mengetahui unjuk kerja aspek *robustness* dan *security* dari skema yang diajukan. Hasilnya menunjukkan bahwa skema yang diajukan memenuhi kriteria *security* dan memiliki tingkat *robustness* yang tinggi yang ditunjukkan dengan perolehan nilai rata-rata rasio akurasi hasil ekstraksi *watermark* sebesar 0,94537.**

***Kata Kunci*— proteksi hak cipta, *watermarking*, *visual cryptography*, citra warna.**

[1]*Program Studi S1 Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia, Jln. Kaliurang Km. 14,5 Yogyakarta 55584 INDONESIA (e-mail: septia.rani@uii.ac.id)*

[2]*Jurusan Ilmu Komputer dan Elektronika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Gadjah Mada, Sekip Utara Bulaksumur Yogyakarta INDONESIA (e-mail: aharjoko@ugm.ac.id)*

I. PENDAHULUAN

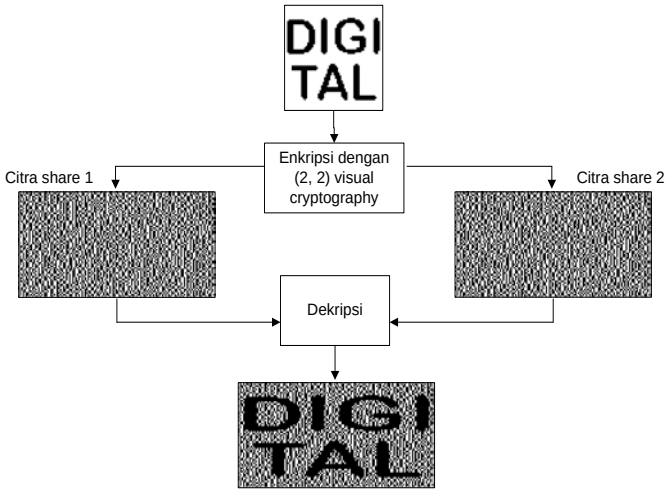
Perkembangan teknologi internet yang semakin pesat telah membuat komunikasi dan pertukaran data menjadi sangat mudah. Berbagai media digital seperti citra, audio, dan video dapat didistribusikan dengan mudah. Kemudahan tersebut memungkinkan seseorang untuk menggandakan, memodifikasi, bahkan menyalahgunakan media digital yang merupakan properti intelektual milik orang lain. Pada kasus seperti ini, proteksi hak cipta terhadap media digital menjadi sesuatu yang penting.

Salah satu mekanisme yang populer yang sudah banyak dikembangkan dan digunakan untuk proteksi hak cipta terhadap citra digital adalah *watermarking*. *Watermarking* sering dikaitkan dengan steganografi, sebab secara prinsip keduanya menggunakan teknik yang tidak jauh berbeda untuk menyisipkan informasi ke dalam data digital [1]. Perbedaan antara keduanya adalah jika pada steganografi informasi rahasia disembunyikan di dalam media digital, yaitu media penampung tidak berarti apa-apa, maka pada *watermarking* justru media digital tersebut yang akan dilindungi kepemilikannya. Pada *watermarking* citra digital, sebuah citra dikombinasikan dengan sebuah *watermark* yang sulit untuk dihilangkan. *Watermark* berfungsi untuk melakukan identifikasi pemilik asli citra. Dengan mekanisme ini, apabila terjadi kasus munculnya keraguan mengenai kepemilikan sebuah citra, pemilik asli citra dapat membuktikan hak cipta kepemilikan dengan melakukan ekstraksi *watermark* dari citra tersebut.

Sebuah skema proteksi hak cipta media digital harus memenuhi beberapa kriteria, yaitu *robustness* (meskipun telah dilakukan serangan-serangan pada media digital, *watermark* yang ditambahkan masih dapat diekstraksi dan diidentifikasi), *imperceptibility* (dengan menggunakan sistem penglihatan manusia, akan sulit dibedakan antara media digital asli dengan media digital yang sudah ditambahkan *watermark*), *security* (hanya pemilik asli media digital yang dapat mengekstrak dan menghilangkan *watermark* yang telah ditambahkan), *blindness* (*watermark* dapat diekstrak tanpa harus menggunakan media digital yang asli), dan *unambiguity* (*watermark* yang diekstraksi dapat dengan jelas memverifikasi pemilik hak cipta dari media digital) [2]. Untuk memenuhi kriteria-kriteria tersebut, telah banyak dikembangkan skema untuk *watermarking*. Pada kebanyakan skema *watermarking*, citra yang akan di-*watermark* (citra *host*) dimodifikasi dengan ditambahkan *watermark* pada domain spasial atau pada domain *transform* [3], [4]. Dengan melakukan modifikasi terhadap citra *host*, kualitas citra dapat dipengaruhi. Bisa jadi penambahan *watermark* dapat menurunkan kualitas citra tersebut. Oleh karena itu, untuk mempertahankan kualitas citra maka dikembangkan skema *lossless watermarking*, yaitu

menambahkan *watermark* tanpa melakukan modifikasi pada citra *host*. Skema *lossless watermarking* yang dikembangkan di antaranya menggunakan teknik *visual cryptography*.

Dalam *visual cryptography*, sebuah citra rahasia dapat dienkripsi menjadi sebanyak n buah citra berbeda yang disebut sebagai citra *share*. Proses dekripsi (*decode*) citra rahasia dapat dilakukan menggunakan sebanyak k buah citra *share* (dengan $k \leq n$) yang masing-masing dicetak pada transparansi dan meletakkan satu transparansi di atas yang lainnya. Jika hanya menggunakan sebanyak $k-1$ buah citra *share* maka proses dekripsi tidak dapat dilakukan. Konsep yang dijelaskan oleh Naor dan Shamir ini dikenal sebagai (k,n) *visual cryptography* [5]. Pada Gbr. 1 ditunjukkan ilustrasi teknik *visual cryptography* dengan nilai $k = 2$ dan $n = 2$.



Gbr. 1 Contoh *visual cryptography* dengan nilai $k = 2$ dan $n = 2$.

Pertama-tama citra rahasia dienkripsi menjadi dua buah citra *share*, kemudian proses dekripsi juga dilakukan menggunakan dua buah citra *share* tersebut. Teknik *visual cryptography* ini dapat diterapkan untuk proteksi hak cipta pada citra digital. Selain dapat mempertahankan kualitas citra yang diproteksi, keuntungan penggunaan teknik *visual cryptography* yaitu dapat memperoleh tingkat keamanan yang tinggi [6].

Beberapa skema proteksi hak cipta untuk citra digital telah dikembangkan menggunakan teknik ini [2], [7], [8]. Secara garis besar, skema proteksi hak cipta untuk citra digital yang dikembangkan pada ketiga penelitian tersebut memiliki langkah-langkah yang sama. Fase pertama adalah pembentukan citra kepemilikan (*ownership share*) dan fase kedua adalah identifikasi kepemilikan melalui ekstraksi *watermark*. Perbedaan di antara ketiganya terletak pada teknik ekstraksi fitur yang digunakan. Pada [2] fitur dari citra diperoleh menggunakan relasi di antara *low sub-band* dan *middle sub-band* koefisien-koefisien wavelet. Pada [7], ekstraksi fitur dilakukan menggunakan *discrete wavelet transform*, *singular value decomposition*, dan digunakan teknik *k-means clustering* untuk mengelompokkan fitur hasil ekstraksi ke dalam dua *cluster*. Sedangkan pada [8], fitur-fitur dari sub-citra diekstraksi menggunakan *fractional* Fourier *transform* dan *singular value decomposition*. Hasil eksperimen menunjukkan bahwa untuk kebanyakan kasus, skema yang diajukan pada [8] memiliki unjuk kerja yang lebih baik dibandingkan skema yang dikembangkan pada [7].

Ketiga penelitian di atas masih menggunakan citra *gray-level* sebagai citra yang akan diproteksi, padahal saat ini citra yang dihasilkan oleh kebanyakan kamera digital berupa citra warna. Oleh karena itu, diperlukan pengembangan skema proteksi hak cipta menggunakan *visual cryptography* untuk citra warna digital. Berdasarkan uraian tersebut, maka pada makalah ini akan dikembangkan skema untuk proteksi hak cipta pada citra warna digital dengan melakukan modifikasi dan perbaikan terhadap skema yang sudah ada yaitu pada [8].

Di dalam makalah ini dipresentasikan skema proteksi hak cipta untuk citra warna digital yang dikembangkan, serta akan dipaparkan hasil pengujian unjuk kerja skema proteksi hak cipta yang diajukan dilihat dari aspek *robustness* dan *security*.

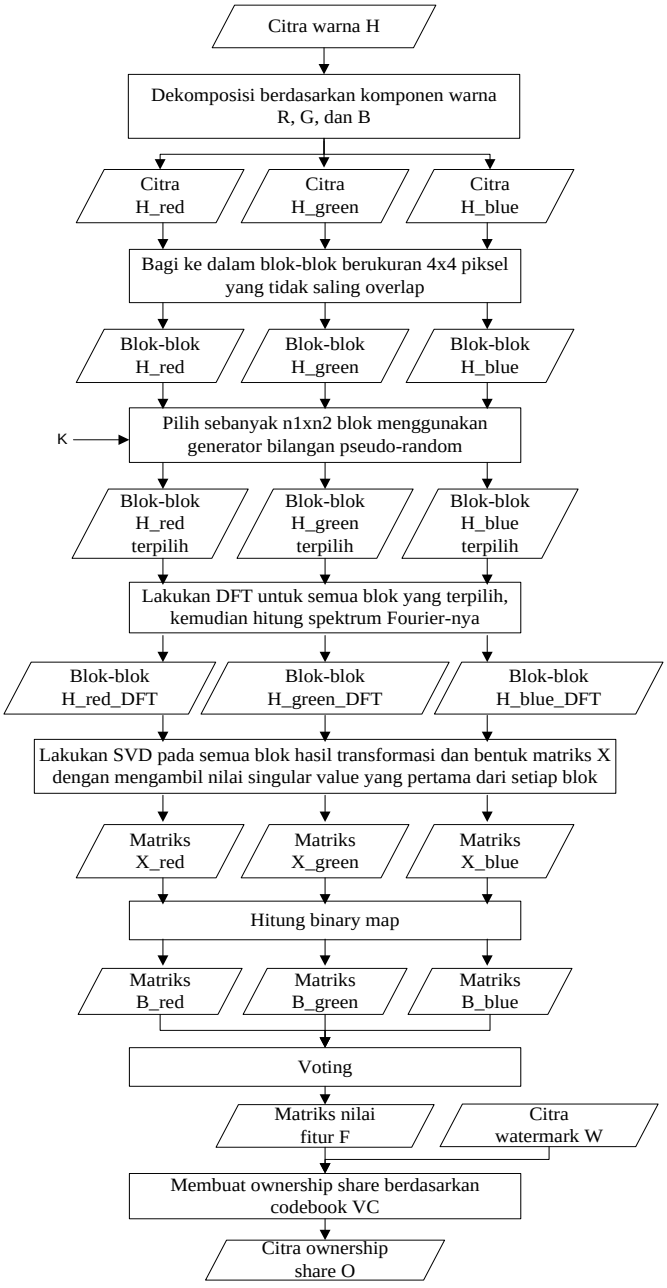
II. METODOLOGI

Pada bagian ini akan dijelaskan secara detail skema proteksi hak cipta yang diajukan. Tahapan proteksi hak cipta pada citra warna menggunakan *visual cryptography* dibagi ke dalam dua fase. Fase pertama adalah pembentukan citra *ownership share* dan fase kedua adalah identifikasi kepemilikan melalui proses ekstraksi *watermark*.

Skema yang digunakan pada makalah ini mengembangkan skema proteksi hak cipta yang diusulkan pada [8]. Terdapat perbedaan pada beberapa tahapan dan metode yang digunakan. Pada penelitian ini terdapat tahapan dekomposisi citra warna dan tahapan *voting*, sedangkan pada skema yang dikembangkan pada [8] tidak terdapat kedua tahapan tersebut. Tahapan dekomposisi citra warna dilakukan karena citra yang akan diproteksi adalah citra warna, sedangkan pada [8] citra yang akan diproteksi adalah citra *gray-level*. Selain itu, metode yang digunakan untuk melakukan transformasi blok-blok yang terpilih ke domain *transform* juga berbeda. Pada makalah ini digunakan metode Fourier *transform*, sedangkan pada [8] digunakan metode *fractional* Fourier *transform*. *Fractional* Fourier *transform* merupakan varian dari Fourier *transform*. Perbedaannya yaitu domain pada Fourier *transform* merupakan murni domain frekuensi, sedangkan domain pada *fractional* Fourier *transform* merupakan kombinasi domain spasial dan frekuensi. Selain itu juga terdapat varian lainnya yaitu *Short Time Fourier Transform* (STFT). Dengan transformasi ini dapat diperoleh analisis frekuensi-waktu [9]. Berdasarkan pertimbangan kompleksitas di antara ketiganya, metode Fourier *transform* merupakan yang paling sederhana sehingga digunakan pada penelitian ini. *Codebook visual cryptography* yang digunakan juga berbeda. Pada penelitian ini untuk setiap piksel pada citra *watermark* akan digantikan dengan 1×2 piksel untuk citra *master share* dan citra *ownership share*-nya, sedangkan pada [8] untuk setiap piksel pada citra *watermark* akan digantikan dengan 2×2 piksel. Adapun untuk tahapan-tahapan lainnya yang digunakan pada skema proteksi hak cipta untuk citra warna digital pada makalah ini sama dengan tahapan-tahapan yang digunakan pada skema yang dikembangkan pada [8].

A. Pembentukan Citra Ownership Share

Tahapan-tahapan untuk proses pembentukan citra *ownership share* dapat dilihat pada Gbr. 2. Citra H merupakan citra warna yang akan diproteksi (citra *host*) dan berukuran $m_1 \times m_2$ piksel, sedangkan citra W merupakan citra biner *watermark* yang berukuran $n_1 \times n_2$ piksel.



Gbr. 2 Tahapan pembentukan citra *ownership share*.

Tahapan-tahapan pembentukan citra *ownership share* adalah sebagai berikut:

1. Melakukan dekomposisi citra warna H berdasarkan komponen warna R (merah), G (hijau), dan B (biru) sehingga diperoleh H_{red}, H_{green}, dan H_{blue}.
2. Mengekstrak fitur citra H_{red}, H_{green}, dan H_{blue}. Proses ekstraksi fitur terdiri atas beberapa langkah sebagai berikut:
   a. Membagi masing-masing citra H_{red}, H_{green}, dan H_{blue} ke dalam blok-blok berukuran 4×4 piksel yang tidak saling *overlap*.
   b. Melakukan pemilihan blok-blok menggunakan generator bilangan *pseudo-random* model Xorshift berdasarkan kunci rahasia *K*. Nilai kunci rahasia *K* akan menjadi *seed* untuk generator bilangan *pseudo-random*. Pemilihan blok-blok dilakukan untuk setiap komponen warna citra pada lokasi yang sama. Jika citra *watermark* yang digunakan berukuran $n_1 \times n_2$ piksel, maka akan dipilih sebanyak $n_1 \times n_2$ blok. Algoritme untuk generator bilangan *pseudo-random* model Xorshift dapat dilihat pada Gbr. 3.

State: x (unsigned 64-bit)
Seed: $x \neq 0$
Update:
$x \wedge (x << a_1) \rightarrow x$
$x \wedge (x >> a_2) \rightarrow x$
$x \wedge (x << a_3) \rightarrow x$
Several sets of a_i produce maximum length PRNGs. We will use set A1: $a_1 = 21$; $a_2 = 35$; $a_3 = 4$

Gbr. 3 Gambar algoritme generator bilangan *pseudo-random* model Xorshift [10].

   c. Melakukan *discrete Fourier transform* (DFT) untuk blok-blok yang terpilih. Proses ini dilakukan dengan menggunakan (1) [11].

$$F(u,v) = \sum_{y=0}^{m-1} \sum_{x=0}^{n-1} f(x,y)(cos\left[2\pi\left(\frac{ux}{n} + \frac{vy}{m}\right)\right] - j\ sin\left[2\pi\left(\frac{ux}{n} + \frac{vy}{m}\right)\right]) \quad (1)$$

dengan m ukuran baris citra dan n ukuran kolom citra. Komponen v bernilai dari 0 sampai dengan $m-1$ dan komponen u bernilai dari 0 sampai dengan $n-1$.
Kemudian dihitung spektrum Fourier-nya menggunakan (2):

$$|F(v,u)| = \sqrt{R^2(v,u) + I^2(v,u)} \quad (2)$$

   d. Melakukan *singular value decomposition* (SVD) pada semua blok hasil transformasi. Kemudian membentuk matriks X dengan mengambil *singular value* yang pertama dari setiap blok. Sampai pada tahap ini akan dihasilkan matriks X_{red}, X_{green}, dan X_{blue}.
   e. Menghitung *binary map* B untuk masing-masing matriks X_{red}, X_{green}, dan X_{blue} menggunakan (3):

$$B_{ij} = \begin{cases} 0 & if\ X_{ij} < X_{avg} \\ 1 & if\ X_{ij} \geq X_{avg} \end{cases} \quad (3)$$

dengan X_{avg} merupakan nilai rata-rata untuk semua piksel di X.

   f. Melakukan *voting* pada ketiga matriks *binary map* B_{red}, B_{green}, dan B_{blue} untuk menghasilkan matriks *feature value* F. Apabila pada lokasi (i,j) berdasarkan matriks B_{red}, B_{green}, dan B_{blue} lebih banyak piksel bernilai 0, maka nilai fitur F pada lokasi (i,j) juga akan bernilai 0. Begitu pula jika lebih banyak piksel bernilai 1, maka nilai fitur F pada lokasi (i,j) akan bernilai 1. Sampai pada proses ini, tahapan ekstraksi fitur telah selesai dilakukan. Dihasilkan matriks nilai fitur F dengan

ukuran $n_1 \times n_2$ sesuai dengan ukuran citra *watermark* yang dipilih.

3. Membentuk citra *ownership share* O menggunakan *codebook visual cryptography* dari informasi matriks nilai fitur F dan *watermark* W. Rancangan *codebook* yang akan digunakan untuk membentuk citra *ownership share* dan citra *master share* dapat dilihat pada Gbr. 4.

- Asumsikan M merupakan citra master share dengan ukuran n_1x$2n_2$ piksel. Kemudian bagi M ke dalam blok-blok berukuran 1x2 piksel yang tidak saling overlap. Isi nilai piksel-piksel dari setiap blok ditentukan dengan aturan pembentukan master share sebagai berikut:
  If (nilai fitur F(i,j) = 1) then nilai piksel untuk M pada blok (i,j) = [1 0]
  If (nilai fitur F(i,j) = 0) then nilai piksel untuk M pada blok (i,j) = [0 1]
- Asumsikan O merupakan citra ownership share dengan ukuran n_1x$2n_2$ piksel. Kemudian bagi O ke dalam blok-blok berukuran 1x2 piksel yang tidak saling overlap. Isi nilai piksel-piksel dari setiap blok ditentukan dengan aturan pembentukan ownership share sebagai berikut:
  If (nilai fitur F(i,j) = 1) and (nilai piksel watermark W(i,j) = 1) then nilai piksel untuk O pada blok (i,j) = [1 0]
  If (nilai fitur F(i,j) = 1) and (nilai piksel watermark W(i,j) = 0) then nilai piksel untuk O pada blok (i,j) = [0 1]
  If (nilai fitur F(i,j) = 0) and (nilai piksel watermark W(i,j) = 1) then nilai piksel untuk O pada blok (i,j) = [0 1]
  If (nilai fitur F(i,j) = 0) and (nilai piksel watermark W(i,j) = 0) then nilai piksel untuk O pada blok (i,j) = [1 0]

Gbr. 4 Gambar rancangan *codebook visual cryptography*.

Codebook visual cryptography yang digunakan dalam makalah ini memodifikasi *codebook* yang digunakan pada [8]. Modifikasi dilakukan dengan mengurangi ukuran blok pengganti, yaitu dengan menghilangkan piksel-piksel pada baris kedua untuk setiap blok *master share* dan *ownership share*. Ukuran blok pengganti yang awalnya 2×2 piksel menjadi 1×2 piksel. Setelah terbentuk citra *ownership share* O, maka selanjutnya citra tersebut didaftarkan pada *certified authority* (CA) untuk proses autentikasi lebih lanjut.

B. Identifikasi Kepemilikan Melalui Proses Ekstraksi Watermark

Apabila terjadi perselisihan atau muncul keraguan mengenai hak kepemilikan citra H', maka pemilik citra harus memberikan nilai kunci K yang tepat agar bisa memunculkan *watermark* untuk membuktikan kepemilikannya terhadap citra H'. Tahapan-tahapan identifikasi kepemilikan adalah sebagai berikut:

1. Melakukan dekomposisi citra warna H' berdasarkan komponen warna R, G, dan B.
2. Mengekstrak fitur dari citra warna H' yang telah didekomposisi sehingga dihasilkan matriks nilai fitur F'. Langkah-langkah untuk proses ekstraksi fitur sama dengan yang dilakukan pada saat fase pembentukan citra *ownership share*.
3. Membentuk citra *master share* M' dari citra H' menggunakan *codebook visual cryptography* dari informasi matriks nilai fitur F'.
4. Melakukan *stacking* antara citra *master share* M' dan citra *ownership share* O (yang disimpan oleh CA) untuk mendapatkan *watermark* W'.
5. Mereduksi ukuran *watermark* W' dengan membagi citra W' ke dalam blok-blok berukuran 1×2 piksel yang tidak saling *overlap* (misalkan dinotasikan dengan blok s'), kemudian untuk setiap blok akan dicari nilai piksel yang dominan menggunakan (4):

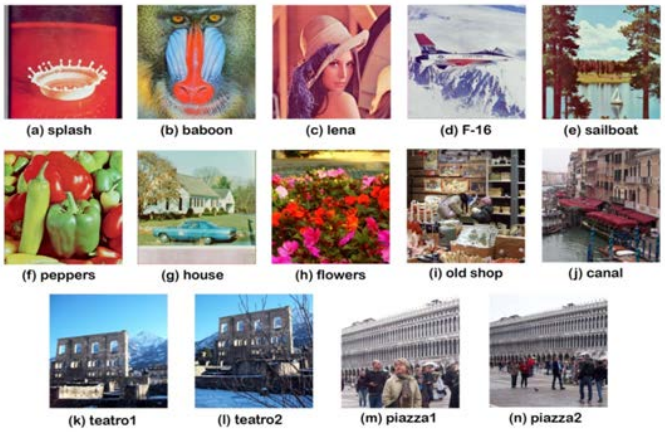
$$W''_{i,j} = \begin{cases} 0 & jika \ \sum_i \sum_j s'_{i,j} < 1 \\ 1 & jika \ \sum_i \sum_j s'_{i,j} \geq 1 \end{cases} \quad (4)$$

Dari proses reduksi diperoleh citra *watermark* W" yang berukuran sama dengan ukuran asli citra *watermark* yaitu berukuran $n_1 \times 2n_2$ piksel. Dari informasi yang terdapat di dalam citra W" dapat diketahui ada atau tidaknya informasi mengenai pemilik citra.

III. HASIL DAN PEMBAHASAN

Beberapa eksperimen dilakukan untuk mengetahui apakah skema proteksi hak cipta berbasis *visual cryptography* yang diajukan memenuhi kriteria-kriteria sebuah skema proteksi hak cipta untuk citra digital. Pada skema proteksi hak cipta yang diajukan, citra *host* yang diproteksi tidak dimodifikasi sama sekali, sehingga kriteria *imperceptibility* dapat dipastikan dipenuhi karena antara citra digital asli dengan citra digital yang telah diproteksi tidak dapat dibedakan. Kriteria *blindness* juga sudah pasti dipenuhi karena pada saat fase identifikasi kepemilikan, proses ekstraksi *watermark* dapat dilakukan tanpa harus menggunakan citra digital yang asli. Kriteria yang relevan untuk diuji pada penelitian ini adalah *robustness*, *security*, dan *unambiguity*.

Data citra *host* yang akan digunakan dalam pengujian terdiri atas 14 buah citra warna 24 bit, masing-masing berukuran 512×512 piksel dan dapat dilihat pada Gbr. 5. Tujuh buah citra diambil dari basis data citra USC-SIPI [12] dan tujuh buah citra yang lainnya diambil menggunakan kamera digital sendiri. Citra (a) – (j) akan digunakan untuk pengujian tingkat *robustness*. Citra (k) – (n) yang merupakan pasangan-pasangan citra yang mirip akan digunakan untuk pengujian *security*. Adapun *watermark* yang digunakan berupa citra biner dengan ukuran 64×64 piksel dan dapat dilihat pada Gbr. 6.



Gbr. 5 Citra untuk pengujian.

Gbr. 6 Citra *watermark*.

Peak signal to noise ratio (PSNR) digunakan untuk mengukur perbandingan kualitas citra asli C dengan citra yang dimodifikasi $\hat{C}$ [8]. PSNR dihitung menggunakan (5):

$$PSNR = 10\ log_{10}\ \frac{255^2}{MSE}\ (dB) \quad (5)$$

Untuk citra berwarna, MSE dihitung menggunakan (6):

$$MSE = \frac{1}{3\times m_1\times m_2}\sum_{h=R,G,B}\sum_{i=1}^{m_1}\sum_{j=1}^{m_2}(C_{hij} - \hat{C}_{hij})^2 \quad (6)$$

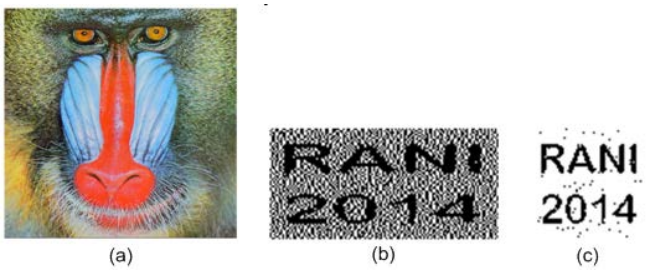
Semakin besar nilai PSNR, secara umum maka berarti semakin kecil distorsi yang terjadi pada citra. Rasio akurasi hasil ekstraksi *watermark* dihitung untuk mengetahui kemiripan antara *watermark* asli W dengan *watermark* hasil ekstraksi $\widehat{W}$. Rasio akurasi hasil ekstraksi *watermark* didefinisikan menggunakan (7):

$$Rasio\ akurasi = \frac{\sum_{i=1}^{n_1}\sum_{j=1}^{n_2}(\overline{W_{ij}\oplus\hat{W}_{ij}})}{n_1\times n_2} \quad (7)$$

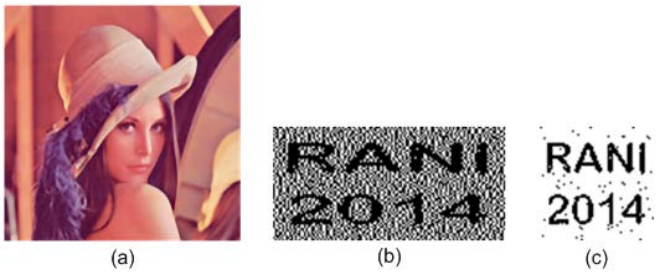
dengan $\oplus$ merupakan operasi eksklusif-OR (XOR) dan $n_1 \times n_2$ merupakan ukuran citra *watermark*. Jika nilai rasio akurasi semakin mendekati 1 maka *watermark* hasil ekstraksi semakin mirip dengan *watermark* asli.

A. Pengujian Aspek Robustness

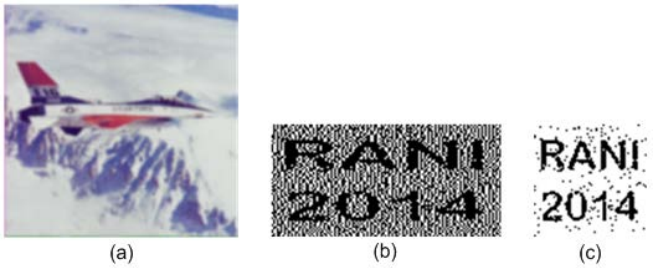
Untuk mengetahui unjuk kerja aspek *robustness* dari skema yang dikembangkan, dilakukan operasi-operasi modifikasi (serangan) pada masing-masing citra *host*. Serangan yang dimaksud adalah *non-malicious attack* yang merupakan operasi tipikal yang umum dilakukan pada pengolahan citra. Serangan-serangan yang dilakukan yaitu kompresi JPEG, *median filtering*, *blurring*, *sharpening*, penambahan *noise*, *resizing*, distorsi, dan rotasi. Digunakan perangkat lunak yang sudah ada untuk melakukan operasi-operasi modifikasi citra tersebut. Gbr. 7 hingga Gbr. 14 menunjukkan hasil yang diperoleh dari percobaan yang dilakukan.



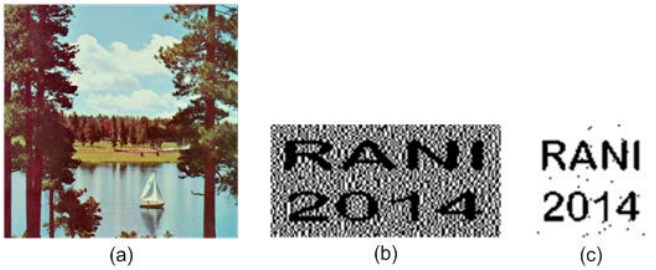
Gbr. 7 (a) Citra "baboon" yang dikompresi (PSNR = 27,3704); (b) *Watermark* hasil ekstraksi; (c) *Watermark* hasil ekstraksi dengan ukuran direduksi (rasio akurasi = 0,9846).



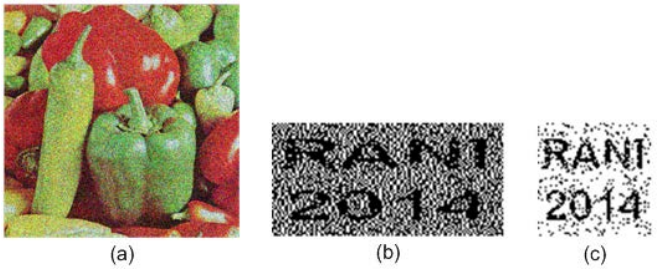
Gbr. 8 (a) Citra "lena" hasil *median filter* (PSNR = 28,7986); (b) *Watermark* hasil ekstraksi; (c) *Watermark* hasil ekstraksi dengan ukuran direduksi (rasio akurasi = 0,9819).



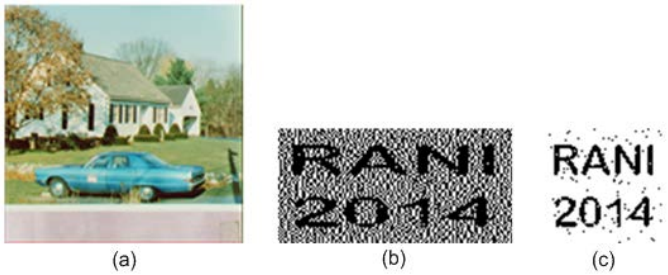
Gbr. 9 (a) Citra "F-16" hasil *blurring* (PSNR = 24,3113); (b) *Watermark* hasil ekstraksi; (c) *Watermark* hasil ekstraksi dengan ukuran direduksi (rasio akurasi = 0,9570).



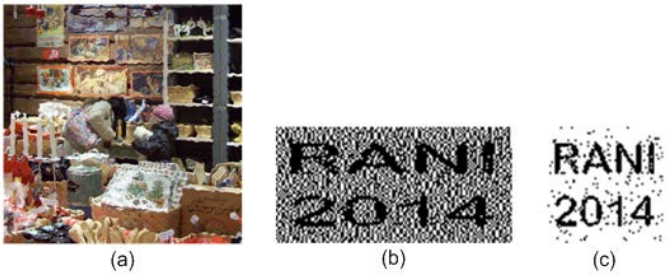
Gbr. 10 (a) Citra "sailboat" hasil *sharpening* (PSNR = 28,0459); (b) *Watermark* hasil ekstraksi; (c) *Watermark* hasil ekstraksi dengan ukuran direduksi (rasio akurasi = 0,9929).



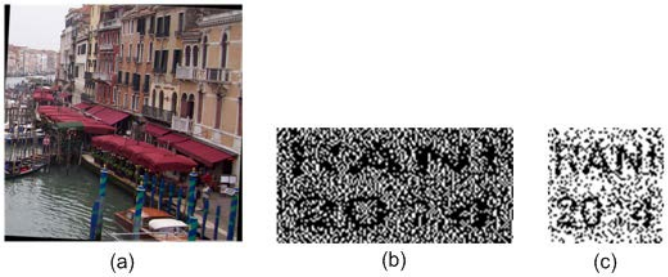
Gbr. 11 (a) Citra "peppers" hasil penambahan *noise* (PSNR = 11,8323); (b) *Watermark* hasil ekstraksi; (c) *Watermark* hasil ekstraksi dengan ukuran direduksi (rasio akurasi = 0,8931).



Gbr. 12 (a) Citra "house" hasil *resizing* (PSNR = 24,2219); (b) *Watermark* hasil ekstraksi; (c) *Watermark* hasil ekstraksi dengan ukuran direduksi (rasio akurasi = 0,9753).



Gbr. 13 (a) Citra "old shop" hasil distorsi (PSNR = 20,4704); (b) *Watermark* hasil ekstraksi; (c) *Watermark* hasil ekstraksi dengan ukuran direduksi (rasio akurasi = 0,9517).



Gbr. 14 (a) Citra "canal" yang dirotasi (PSNR = 13,1850); (b) *Watermark* hasil ekstraksi; (c) *Watermark* hasil ekstraksi dengan ukuran direduksi (rasio akurasi = 0,7742).

Penjelasan untuk masing-masing serangan yang dilakukan adalah sebagai berikut:

1. Kompresi JPEG. Citra *host* dikompres menggunakan JPEG dengan faktor kualitas 50%. PSNR dari citra "baboon" yang dikompresi adalah 27,3704 dB dan rasio akurasi *watermark* hasil ekstraksinya adalah 0,9846.
2. *Median filtering*. Dilakukan *median filtering* dengan radius sebesar 3 piksel pada citra *host*. PSNR dari citra "lena" hasil serangan *median filtering* adalah 28,7986 dB dan rasio akurasi *watermark* hasil ekstraksinya sebesar 0,9819.
3. *Blurring*. Dilakukan serangan *blurring* menggunakan *Gaussian blur* dengan radius sebesar 3 piksel pada citra *host*. PSNR dari citra "F-16" hasil dari serangan *blurring* adalah 24,3113 dB dan rasio akurasi *watermark* hasil ekstraksinya sebesar 0,9570.
4. *Sharpening*. Dilakukan serangan *sharpening* pada citra *host* menggunakan perangkat lunak Adobe Photoshop CS3. PSNR dari citra "sailboat" hasil dari serangan *sharpening* adalah 28,0459 dB dan rasio akurasi *watermark* hasil ekstraksinya sebesar 0,9929.
5. Penambahan *noise*. Dilakukan serangan dengan melakukan penambahan 30% *noise Gaussian* pada citra asli. PSNR dari citra "peppers" hasil dari serangan penambahan *noise* adalah 11,8323 dB dan rasio akurasi *watermark* hasil ekstraksinya sebesar 0,8931.
6. *Resizing*. Pertama-tama dilakukan *downscale* pada citra yang awalnya berukuran 512×512 piksel ke 128×128 piksel. Kemudian citra di-*upscale* sehingga kembali ke ukuran asli yaitu 512×512 piksel. PSNR dari citra "house" hasil dari serangan *resizing* adalah 24,2219 dB dan rasio akurasi *watermark* hasil ekstraksinya sebesar 0,9753.
7. Distorsi. Serangan distorsi dilakukan dengan menggunakan efek *ripple*. PSNR dari citra "old shop" hasil dari serangan distorsi adalah 20,4704 dB dan rasio akurasi *watermark* hasil ekstraksinya sebesar 0,9517.
8. Rotasi. Citra *host* dirotasi sebesar 3º searah dengan jarum jam. PSNR dari citra "canal" yang dirotasi adalah 13,1850 dB dan rasio akurasi *watermark* hasil ekstraksinya adalah 0,7742.

Tabel I menunjukkan hasil pengujian untuk semua operasi serangan citra. Dapat dilihat bahwa nilai rata-rata rasio akurasi *watermark* hasil ekstraksi untuk semua jenis serangan pemrosesan citra yang dilakukan adalah mendekati 1. Hal ini menunjukkan bahwa skema proteksi hak cipta untuk citra warna digital yang diajukan *robust* terhadap berbagai operasi serangan pemrosesan citra. *Watermark* dapat diperoleh kembali dengan nilai rata-rata rasio akurasi sebesar 0,99092 meskipun dilakukan serangan kompresi JPEG dengan faktor kualitas 50% pada citra *host*. Nilai rata-rata rasio akurasi paling rendah diperoleh ketika dilakukan serangan rotasi pada citra *host*, yaitu sebesar 0,82431.

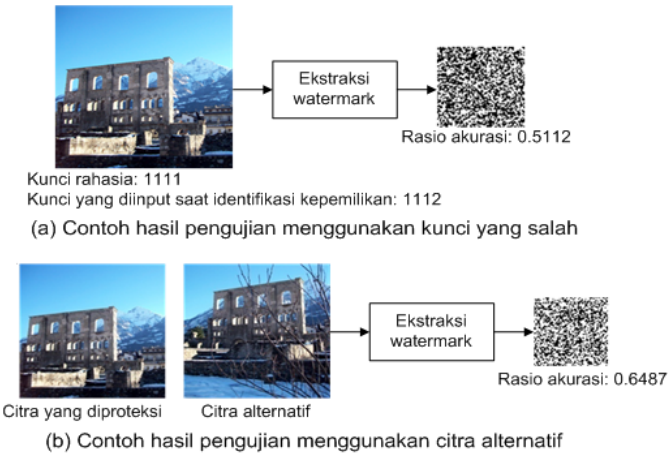
Pada pengujian dilakukan verifikasi dengan mengecek apakah *watermark* yang diekstraksi sudah sesuai dengan *watermark* asli. Kemudian dihitung nilai rasio akurasi untuk mengetahui tingkat kemiripan antara *watermark* hasil ekstraksi dengan *watermark* asli. Berdasarkan hasil pengecekan diperoleh nilai rasio akurasi yang mendekati 1. Hal ini menunjukkan bahwa *watermark* hasil ekstraksi mirip dan sudah sesuai dengan *watermark* asli. Dari proses pengecekan yang telah dilakukan ini menunjukkan bahwa skema proteksi hak cipta untuk citra warna digital yang diajukan memenuhi kriteria *unambiguity*.

TABEL I
HASIL PENGUJIAN TERHADAP SERANGAN PEMROSESAN CITRA

No	Nama serangan	Nilai rata-rata rasio akurasi *watermark* hasil ekstraksi
1	Kompresi JPEG	0,99092
2	*Median filtering*	0,96496
3	*Blurring*	0,94511
4	*Sharpening*	0,98706
5	Penambahan *noise*	0,90791
6	*Resizing*	0,97567
7	Distorsi	0,96699
8	Rotasi	0,82431

B. *Pengujian Aspek Security*

Untuk mengetahui *security* dari skema yang dikembangkan terdapat beberapa skenario pengujian. Pada skenario pertama dilakukan pengujian dengan memasukkan kunci K yang salah pada saat proses identifikasi kepemilikan. Pada skenario kedua dilakukan pengujian menggunakan citra alternatif yang mirip dengan citra asli yang diproteksi. Pada Gbr. 15 dapat dilihat contoh hasil pengujian aspek *security*.



Gbr. 15 Contoh hasil pengujian aspek *security*.

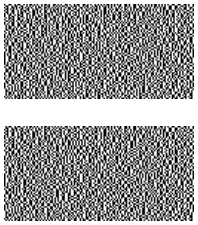
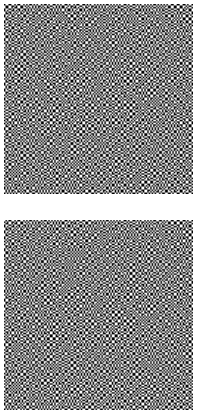
Jika dimasukkan kunci yang salah pada saat identifikasi kepemilikan, maka *watermark* hasil ekstraksi yang dihasilkan

berupa titik-titik yang tidak memiliki arti. Demikian pula jika digunakan citra alternatif, maka *watermark* hasil ekstraksi yang dihasilkan juga berupa titik-titik seperti *noise*. Dengan menggunakan skema proteksi hak cipta yang dikembangkan, *user* tidak dapat mengklaim citra lain yang bukan miliknya.

C. Pengujian Pengaruh Visual Cryptography yang Digunakan

Untuk mengetahui pengaruh *visual cryptography* yang digunakan, dilakukan pengujian dengan membandingkan hasilnya dengan mengimplementasikan *codebook* yang digunakan pada [8]. Pada Tabel II dapat dilihat perbandingan hasil yang diperoleh. Hasil akhir ekstraksi *watermark* dari keduanya identik dan memiliki nilai rasio akurasi yang sama. Meskipun demikian, *codebook visual cryptography* pada penelitian ini lebih efisien karena dapat memperkecil ukuran citra *ownership share* sehingga dapat mengurangi media untuk penyimpanannya.

TABEL II
PERBANDINGAN PENGGUNAAN *CODEBOOK VISUAL CRYPTOGRAPHY*

Percobaan menggunakan *codebook* VC penelitian ini	**Percobaan menggunakan *codebook* VC pada [8]**
Citra *ownership share* dan *master share*: 	Citra *ownership share* dan *master share*: 
Hasil *stacking* dan *watermark* hasil ekstraksi:  Rasio akurasi: 0,9651	Hasil *stacking* dan *watermark* hasil ekstraksi:  Rasio akurasi: 0,9651

D. Perbandingan Unjuk kerja dengan Skema Proteksi Hak Cipta Lain

Pada Tabel III ditunjukkan perbandingan unjuk kerja ditinjau dari aspek *robustness* antara skema proteksi hak cipta untuk citra warna digital yang diajukan pada makalah ini dengan skema proteksi hak cipta berbasis *visual cryptography* yang diajukan pada [8]. Skema yang diajukan pada [8] menggunakan citra *gray-level* sebagai citra yang akan diproteksi, sedangkan skema yang diajukan pada makalah ini menggunakan citra warna. Metode pada [8] diimplementasikan kemudian pengujiannya dilakukan dengan mengkonversi data citra warna ke citra *gray-level*.

TABEL III
PERBANDINGAN NILAI RATA-RATA RASIO AKURASI DENGAN SKEMA PROTEKSI HAK CIPTA [8]

Serangan	**Skema [8]**	**Skema yang diajukan pada penelitian ini**
Kompresi JPEG	0,99620	0,99092
Median filtering	0,96296	0,96496
Blurring	0,94098	0,94511
Sharpening	0,98792	0,98706
Penambahan *noise*	0,91746	0,90791
Resizing	0,97349	0,97567
Distorsi	0,96544	0,96699
Rotasi	0,81499	0,82431
Nilai rata-rata (untuk semua serangan)	0,94493	0,94537

Pengujian terhadap serangan kompresi JPEG, *median filtering*, *blurring*, *sharpening*, penambahan *noise*, *resizing*, distorsi, dan rotasi masing-masing menggunakan 10 buah citra. Berdasarkan Tabel III, dalam menghadapi serangan *median filtering*, *blurring*, *resizing*, distorsi, dan rotasi, skema proteksi hak cipta yang diajukan memiliki nilai rata-rata rasio akurasi yang relatif lebih baik. Sedangkan untuk tiga buah serangan yang lainnya, yaitu kompresi JPEG, *sharpening*, dan penambahan *noise*, nilai rata-rata rasio akurasinya tidak lebih baik. Dari perbandingan yang telah dilakukan dapat disimpulkan bahwa secara keseluruhan skema yang diajukan memiliki unjuk kerja *robustness* yang relatif lebih baik daripada skema yang diajukan pada [8]. Hal ini ditunjukkan dengan nilai rata-rata rasio akurasi untuk semua serangan yang besarnya 0,94537, yang nilai tersebut 0,00044 lebih tinggi dibandingkan dengan hasil yang diperoleh dari skema pada [8].

IV. KESIMPULAN DAN SARAN

Dari pembahasan yang telah dipaparkan dapat diambil beberapa kesimpulan. Pada makalah ini, kontribusi utama yang dilakukan adalah mengembangkan skema proteksi hak cipta yang diajukan pada penelitian sebelumnya untuk diterapkan pada citra warna digital. Teknik *visual cryptography* dipilih karena mudah diimplementasikan, memiliki tingkat keamanan yang tinggi, dan juga dapat mempertahankan kualitas citra yang diproteksi. Skema proteksi hak cipta untuk citra warna digital menggunakan *visual cryptography* yang diajukan *robust* terhadap berbagai operasi serangan pemrosesan citra (*non-malicious attack*), di antaranya serangan kompresi JPEG, *median filtering*, *blurring*, *sharpening*, penambahan *noise*, *resizing*, dan distorsi. Skema yang diajukan juga memenuhi kriteria *security*. *Codebook visual cryptography* yang digunakan lebih efisien dibandingkan dengan yang digunakan pada penelitian sebelumnya. Dengan menghilangkan piksel-piksel pada baris

kedua untuk setiap blok pengganti pada citra *master share* dan citra *ownership share* maka ukuran *file* citra *ownership share* yang akan disimpan pada *certified authority* dapat diperkecil.

Adapun saran untuk penelitian lebih lanjut, selain melakukan proteksi dari sisi hak cipta untuk citra warna digital, juga perlu dikembangkan sistem yang dapat melakukan proteksi dari sisi objeknya agar citra warna digital tidak dapat digandakan ataupun dimodifikasi oleh orang lain. Di samping itu juga dapat dilakukan pengembangan penelitian dengan menggunakan data citra medis atau citra satelit sebagai data uji.

REFERENSI

[1] Dewanto, W., Susanto, M. F., dan Sumaryono, S., "Penyisipan Kode Dalam Sinyal Iklan Radio Siaran Niaga Sebagai Penanda Identitas Kepemilikan", *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*, vol. 1(1), hal. 54-58, 2012.

[2] Lou, D., Tso, H. dan Liu, J., "A Copyright Protection Scheme for Digital Images using Visual Cryptography Technique", *Computer Standards & Interfaces*, vol. 29, hal. 125–131, 2007.

[3] Ali, M., Ahn, C.W., Pant, M. dan Siarry, P., "An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony", *Information Sciences*, vol. 301, hal. 44-60, 2015.

[4] Qi, X. dan Xin, X., "A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization", *Journal of Visual Communication and Image Representation*, vol. 30, hal. 312-327, 2015.

[5] Naor, M. dan Shamir, A., "Visual Cryptography", *Proceedings of Advances in Cryptology: Eurocrypt'94*, LNCS 950, hal. 1-12, 1995.

[6] Liu, F. dan Wu, C., "Robust Visual Cryptography-Based Watermarking Scheme for Multiple Cover Images and Multiple Owners", *IET Information Security*, vol. 5, hal. 121–128, 2011.

[7] Wang, M. dan Chen, W., "A Hybrid DWT-SVD Copyright Protection Scheme Based on k-means Clustering and Visual Cryptography", *Computer Standards & Interfaces*, vol. 31, hal. 757–762, 2009.

[8] Rawat, S. dan Raman, B., "A Blind Watermarking Algorithm Based on Fractional Fourier Transform and Visual Cryptography", *Signal Processing*, vol. 92, hal. 1480–1491, 2012.

[9] Puspasari, I., "Analisis Non-Stasioner pada Deteksi Non-Invasive Sinyal Suara Jantung Koroner", *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*, vol. 4(2), 2015.

[10] Evans, H. (2010) PHYSICS P410/P609: Pseudo-Random Number Generators. [Online], *http://hep.physics.indiana.edu/~hgevans/p410-p609/material/04_rand/prng_types.html*, tanggal akses: 16 Juni 2014.

[11] Kadir, A. dan Susanto, A., *Teori dan Aplikasi Pengolahan Citra*, Penerbit ANDI, Yogyakarta, 2013.

[12] The USC-SIPI Image Database. (1977) Volume 3: Miscellaneous. [Online], *http://sipi.usc.edu/database/database.php?volume=misc*, tanggal akses: 15 April 2014.