

**IDENTIFIKASI GAMBAR DIGITAL UNTUK MENGETAHUI  
KEASLIAN GAMBAR DENGAN METODE *INCONSISTENT SHADOW***

**(Skripsi)**

Oleh

**Fahmi Meitra Hidayat**



**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM  
UNIVERSITAS LAMPUNG  
BANDAR LAMPUNG  
2018**

**ABSTRACT****DIGITAL IMAGE IDENTIFICATION TO FIND  
THE ORIGINALITY OF THE IMAGE WITH INCONSISTENT SHADOW****By****FAHMI MEITRA HIDAYAT**

Nowadays, modifying a digital image is very easy, with the release of any photo editing software we can easily change an image so that the value of an image when used as evidence in court is not strong. There is a method of forensic photograph in the literature (Inconsistent shadow) that detects image tampering through the shadow of the image with geometry, but the accuracy is not tested with another method. Therefore it is necessary to have a research to determine the accuracy of that method. We use a robust algorithm which is one of the techniques used in forensic photographs to group a point and also the Hausdorff distance method to calculate the comparative distance of a set of pixels in an image. The method will be compared with the Inconsistent shadow method to find its accuracy. The test was done by examining thirty-five images that have been modified. Inconsistent shadow method managed to detect fake images with 80% percent while robust algorithm method had a better percentage of 91% for 10 constraints. However, in the case of constraints greater than 50 Inconsistent shadow method is better with 100% percentage while robust algorithm method remains at 91%.

Keywords : *image forensic, image forgery, photo forensic, robust algorithm.*

## ABSTRAK

### IDENTIFIKASI GAMBAR UNTUK MENGETAHUI KEASLIAN GAMBAR DENGAN METODE *INCONSISTENT SHADOW*

Oleh

**FAHMI MEITRA HIDAYAT**

Saat ini memodifikasi sebuah gambar digital sangatlah mudah, dengan beredarnya software foto editing siapapun bisa dengan mudah merubah sebuah gambar sehingga nilai suatu gambar saat dijadikan barang bukti di pengadilan tidaklah kuat. Terdapat suatu metode foto forensik yang ada di literatur yaitu metode *Inconsistent shadow* yang mendeteksi pemalsuan gambar melalui bayangan pada gambar secara geometris namun pada penelitiannya belum bisa diuji ketepatan metodenya. Oleh karena itu perlu adanya suatu penelitian untuk menentukan seberapa besar akurasi dari metode *Inconsistent shadow*. Dengan menggunakan *robust algorithm* yang merupakan salah satu teknik yang digunakan dalam foto forensik untuk mengelompokkan suatu titik dan juga metode *Hausdorff distance* untuk menghitung jarak perbandingan nilai sekumpulan *pixel* pada gambar. Metode tersebut akan dibandingkan dengan metode *Inconsistent shadow* untuk menemukan akurasi. Pengujian dilakukan dengan mengujikan tiga puluh dua gambar yang telah dimodifikasi, metode *Inconsistent shadow* berhasil mendeteksi gambar palsu dengan persentasi 80% sedangkan metode *robust algorithm* memiliki persentasi lebih baik yaitu 91% untuk 10 kendala. Namun pada kasus kendala yang lebih besar dari 50 metode *Inconsistent shadow* lebih unggul dengan persentasi 100% sedangkan metode *robust algorithm* tetap pada 91%.

Kata Kunci : *foto forensic, image forensic, image forgery, robust algorithm,*

**IDENTIFIKASI GAMBAR DIGITAL UNTUK  
MENGETAHUI KEASLIAN GAMBAR DENGAN  
METODE INCONSISTENT SHADOW**

Oleh

**FAHMI MEITRA HIDAYAT**

**Skripsi**

Sebagai Salah Satu Syarat Untuk Memperoleh Gelar  
SARJANA KOMPUTER

pada

Jurusan Ilmu Komputer  
Fakultas Matematika dan Ilmu Pengetahuan Alam



**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM  
UNIVERSITAS LAMPUNG  
BANDAR LAMPUNG  
2018**

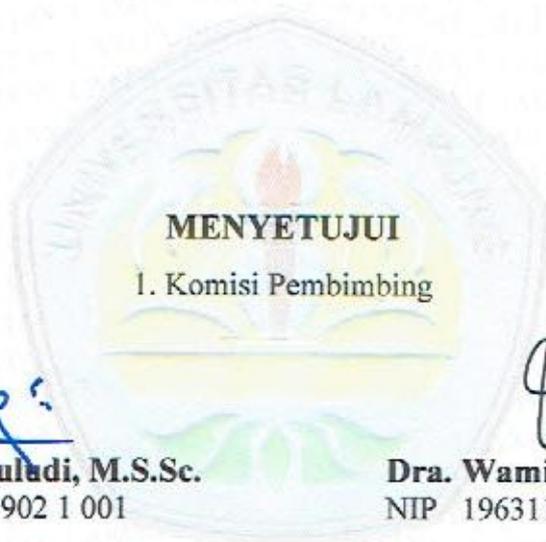
Judul Skripsi : **IDENTIFIKASI GAMBAR DIGITAL UNTUK MENGETAHUI KEASLIAN GAMBAR DENGAN METODE *INCONSISTENT SHADOW***

Nama Mahasiswa : **Fahmi Meitra Hidayat**

No. Pokok Mahasiswa : 1317051021

Jurusan : Ilmu Komputer

Fakultas : Matematika dan Ilmu Pengetahuan Alam



**Dr. Ir. Kurnia Muludi, M.S.Sc.**  
NIP 19640616 198902 1 001

**Dra. Wamiliana, M.A., Ph.D.**  
NIP 19631108 198902 2 001

2. Mengetahui  
Ketua Jurusan Ilmu Komputer  
FMIPA Universitas Lampung

**Dr. Ir. Kurnia Muludi, M.S.Sc.**  
NIP 19640616 198902 1 001

**MENGESAHKAN**

1. Tim Penguji

Ketua : **Dr. Ir. Kurnia Muludi, M.S.Sc.** .....

*Kurnia Muludi S.*

Sekretaris : **Dra. Wamiliana, M.A., Ph.D.** .....

*[Signature]*

Penguji  
Bukan Pembimbing : **Dwi Sakethi, S.Si., M.Kom.** .....

*[Signature]*

2. Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam



*[Signature]*  
**Prof. Warsito, S.Si. D.E.A., Ph.D.**  
NIP 19710212 199512 1 001

Tanggal Lulus Ujian Skripsi : 01 Februari 2018

## PERNYATAAN

Saya yang bertanda tangan di bawah ini, menyatakan bahwa skripsi saya yang berjudul “Identifikasi Gambar Digital Untuk Mengetahui Keaslian Gambar Dengan Metode *Inconsistent Shadow*” merupakan karya saya sendiri dan bukan hasil karya orang lain. Semua tulisan yang tertuang di skripsi ini telah mengikuti kaidah penulisan karya ilmiah Universitas Lampung. Apabila di kemudian hari terbukti bahwa skripsi saya merupakan hasil penjiplakan atau dibuat orang lain, maka saya bersedia menerima sanksi berupa pencabutan gelar yang telah saya terima.

Bandar Lampung, 01 Februari 2018



**Fahmi Meitra Hidayat**  
NPM. 1317051021

## RIWAYAT HIDUP



Penulis dilahirkan pada tanggal 5 Mei 1995 di Gisting, Tanggamus. Penulis merupakan anak pertama dari tiga bersaudara dengan ayah bernama Samsul Hilal dan ibu bernama Irdiyati. Penulis menyelesaikan pendidikan formal pertama kali di SD Negeri 1 Banding Agung tahun 2007, kemudian melanjutkan pendidikan menengah pertama di SMP Negeri 1 Talang Padang dan selesai pada tahun 2010. Pendidikan menengah atas di SMA Al-Kautsar Bandar Lampung diselesaikan penulis pada tahun 2013.

Pada tahun 2013, penulis terdaftar sebagai mahasiswa Jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung melalui jalur SNMPTN. Pada bulan Februari tahun 2016, penulis melakukan Kerja Praktik di Grapari Telkomsel Lampung. Pada bulan Juli tahun 2016 penulis melaksanakan Kuliah Kerja Nyata di Desa Kalidadi Kecamatan Gadingrejo Kabupaten Pringsewu. Selama menjadi mahasiswa, penulis cukup aktif berorganisasi, diantaranya adalah:

1. Anggota Bidang Kaderisasi Badan Eksekutif Mahasiswa FMIPA Unila pada tahun periode 2014-2015.

2. Anggota Bidang Kaderisasi Himpunan Mahasiswa Jurusan Ilmu Komputer pada tahun periode 2014-2015.
3. Kepala Bidang Media Informasi Mahasiswa Jurusan Ilmu Komputer pada tahun periode 2015-2016.
4. Asisten Laboratorium dan Asisten Dosen Jurusan Ilmu Komputer pada tahun periode 2014-2017.

## **PERSEMBAHAN**

*Puji dan syukur ku ucapkan kepada Allah SWT atas segala nikmat dan karunia-Nya sehingga skripsi ini dapat terselesaikan.*

*Ku persembahkan tulisan ini pada :*

*Bapak dan ibuku*

*Yang selalu mengajarku banyak hal*

*Yang selalu memberiku dukungan terbaik*

*Yang kasih dan sayangnya tak kan sanggup tuk kubalas*

*Adik adikku serta seluruh keluarga yang telah memberikan dukungan*

*Keluarga besar Ilmu Komputer Unila*

*Serta Almamater tercinta,*

*Universitas Lampung.*

**MOTTO**

“The way your heart sounds makes all the difference,  
it's what decides if you'll endure the pain that we all feel.  
The way your heart beats, makes all the difference in learning to live.  
Spread before you is your soul, so forever hold the dreams within our hearts.  
Through nature's inflexible grace.  
I'm learning to live.  
(John Myung)

## SANWACANA

Puji dan syukur penulis ucapkan kehadiran Allah SWT atas segala rahmat, hidayah dan kesehatan yang diberikan kepada penulis sehingga dapat menyelesaikan penulisan skripsi ini.

Skripsi ini disusun sebagai syarat untuk memperoleh gelar Sarjana Komputer di Jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Universitas Lampung. Judul dari skripsi ini adalah “Identifikasi Gambar Digital Untuk Mengetahui Keaslian Gambar Dengan Metode *Inconsistent Shadow*”.

Dalam penyusunan skripsi ini, penulis banyak menghadapi kesulitan. Namun, berkat bantuan dan dorongan dari berbagai pihak, akhirnya penulis dapat menyelesaikan skripsi ini. Untuk itu pada kesempatan ini, penulis mengucapkan terimakasih kepada:

1. Kedua orang tua, Bapak Samsul Hilal dan Ibu Irdayati, adik-adikku tercinta Fadli Alvindra dan Fania Ainur Ramadiani, serta keluarga besar yang selalu memberikan doa, motivasi dan kasih sayang yang tak terhingga.
2. Bapak Dr. Ir. Kurnia Muludi, M.S.Sc. sebagai pembimbing I, yang telah membimbing penulis dan memberikan ide, kritik serta saran sehingga penulisan skripsi ini dapat diselesaikan.
3. Ibu Prof. Dr. Dra. Wamiliana, M.A., Ph.D. sebagai pembahas I, yang telah memberikan saran, bantuan dan membimbing penulis dalam pembuatan skripsi ini.

4. Bapak Dwi Sakethi, S.Si., M.Kom. sebagai pembahas II, yang telah memberikan masukan-masukan yang bermanfaat dalam perbaikan skripsi ini.
5. Bapak dan Ibu Dosen serta seluruh staff Jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung yang telah memberikan ilmu dan pengalaman dalam hidup untuk menjadi lebih baik.
6. Seluruh anggota grup Coding dan grup Jaja Miharja (2018) yang menjadi pemicu penulis dalam menyelesaikan skripsi ini. Tanpa kalian mungkin penulis masih malas mengerjakan skripsi ini walau terkadang kalian lah yang membuat penulis menjadi malas.
7. Keluarga besar mahasiswa Ilmu Komputer Unila khususnya angkatan 2013 yang berjuang bersama dalam suka maupun duka selama di Universitas Lampung. Kebersamaan yang telah dilalui menjadi pengalaman berharga bagi penulis.
8. *Last but not least*, Oktarini Husaini, S.Si. yang telah membantu penulis menyelesaikan perkuliahannya di Universitas Lampung, banyak sekali kontribusi yang tak mungkin disebutkan satu persatu.

Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan, akan tetapi sedikit harapan semoga skripsi ini bermanfaat bagi perkembangan ilmu pengetahuan terutama bagi teman-teman Ilmu Komputer.

Bandar Lampung, 1 Februari 2018

Fahmi Meitra Hidayat

## DAFTAR ISI

	Halaman
DAFTAR ISI.....	xiii
DAFTAR GAMBAR .....	xv
DAFTAR TABEL.....	xvi
I. PENDAHULUAN .....	1
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah .....	2
1.3. Batasan Masalah.....	2
1.4. Tujuan Penelitian.....	3
1.5. Manfaat Penelitian.....	3
II. TINJAUAN PUSTAKA.....	4
2.1. Pengolahan Citra Digital .....	4
2.2. Foto Forensik.....	5
2.3. <i>Digital Image Forensic</i> .....	5
2.4. <i>Resampling</i> .....	6
2.5. Pemalsuan gambar.....	6
2.5.1. <i>Image Retouching</i> .....	6
2.5.2. <i>Splicing</i> .....	7
2.5.3. <i>Cloning</i> .....	7
2.6. Bayangan .....	7
2.7. Teknik Mendeteksi Pemalsuan Gambar.....	10
2.8. Teknik Mendeteksi Sumber Gambar.....	10
2.9. <i>Anti Forensic</i> .....	13
2.10. <i>Confusion Matrix</i> .....	14
2.11. <i>Robust Algorithm</i> .....	15

III. METODE PENELITIAN.....	16
3.1. Waktu dan Tempat .....	16
3.2. Alat dan Bahan .....	16
3.3. Tahap Penelitian .....	17
IV. HASIL DAN PEMBAHASAN .....	27
4.1. <i>Blurring</i> .....	27
4.2. <i>Color quantization</i> .....	28
4.3. <i>Robust Algorithm</i> .....	28
4.4. <i>Testing</i> .....	33
V. KESIMPULAN .....	35
5.1. Kesimpulan.....	35
5.2. Saran.....	36
DAFTAR PUSTAKA .....	

## DAFTAR GAMBAR

	Halaman
Gambar 1. Bayangan yang terbentuk pada gambar .....	9
Gambar 2. <i>Flowchart</i> alur metodologi penelitian .....	17
Gambar 3. <i>Cast and attached shadow</i> .....	19
Gambar 4. Gambar irisan <i>constraint</i> .....	20
Gambar 5. Potongan kode pada proses <i>blurring</i> .....	27
Gambar 6. Hasil <i>blurring</i> .....	27
Gambar 7. Potongan kode pada proses <i>color quantization</i> .....	28
Gambar 8. Hasil <i>color quantization</i> .....	28
Gambar 9. Potongan kode pada proses pengelompokan blok.....	29
Gambar 10. Potongan kode pada proses pengurutan blok .....	29
Gambar 11. Potongan kode pada proses ekstraksi blok.....	29
Gambar 12. Potongan kode pada proses penggabungan blok.....	30
Gambar 13. Potongan kode pada proses <i>Hausdorff distance</i> .....	30
Gambar 14. Potongan kode pada proses penandaan gambar .....	31
Gambar 15. Hasil <i>Robust algorithm</i> .....	31
Gambar 16. Hasil jika gambar dideteksi telah dimodifikasi .....	32
Gambar 17. Hasil jika gambar tidak berhasil dideteksi .....	32
Gambar 18. Hasil jika gambar yang salah dapat dideteksi .....	33

**DAFTAR TABEL**

	Halaman
Tabel 1. Akurasi Dari Algoritma Robust .....	34
Tabel 2. Perbandingan Algoritma Robust Dengan <i>Inconsistent Shadow</i> .....	34

## I. PENDAHULUAN

### 1.1. Latar Belakang

Gambar memiliki nilai lebih dari seribu kata yang dapat mewakili berbagai kata yang ingin disampaikan. Gambar juga dapat menjadi sangat ampuh dalam menyampaikan pesan melebihi kata kata jika digunakan dengan cerdas. Buktinya saja di sepanjang jalan lebih sering ditemukan banyak gambar dengan kata yang sedikit. Pemasang gambar pasti paham bahwa para pengguna jalan tidak punya waktu untuk membaca kata kata yang panjang.

Gambar digital pada saat ini sudah sangat sering digunakan seperti foto, piagam, dokumen, dan lainnya. Dengan semakin maraknya penggunaan gambar digital maka semakin banyak pula cara untuk mengganti, menghapus, dan menduplikasi gambar tersebut secara ilegal.

Banyaknya gambar yang beredar di internet saat ini sangat sulit untuk dipercaya. Gambar yang telah dimodifikasi banyak ditampilkan seperti di majalah, kampanye partai, serangan politik, jurnal ilmiah, bahkan berita *hoax* yang ada di dalam *email*. Gambar yang dimodifikasi berkembang dengan cepat dan canggih, bahkan para ahli sering tidak bisa mengandalkan pengamatan visual untuk membedakan gambar asli dan gambar yang telah dipalsukan.

Dengan adanya tindakan dan cara untuk mengetahui keaslian gambar maka dapat diberikan bukti - bukti yang baik. Gambar yang diidentifikasi sebagai gambar yang telah dimanipulasi akan ditemukan beberapa kejanggalan – kejanggalan seperti refleksi dari objek yang ada di dalam gambar tidak konsisten serta terdapat perbedaan warna antara objek satu dan lainnya.

Berdasarkan penelitian Farid (2009) yang membahas tentang *image forensic* dijelaskan berbagai metode untuk mendeteksi pemalsuan gambar yang salah satu metodenya adalah *Inconsistent shadow*, metode yang tidak memerlukan data mentah gambar sebagai dasar penelitian dalam mendeteksi pemalsuan gambar melainkan menggunakan bayangan pada gambar sebagai data dalam mendeteksi pemalsuan gambar. Tetapi dalam penelitiannya tersebut belum terdapat perbandingan dengan metode yang lain sehingga persentase ketepatannya masih diragukan. Dalam penelitian ini penulis tertarik untuk mengkaji lebih lanjut tentang mengetahui seberapa optimal metode *Inconsistent shadow* untuk mendeteksi gambar yg telah dimodifikasi dengan teknik *copy move*.

### **1.2. Rumusan Masalah**

Rumusan masalah dalam penelitian ini adalah untuk mengetahui akurasi ketepatan metode *Inconsistent shadow*.

### **1.3. Batasan Masalah**

Batasan masalah dari penelitian ini adalah sebagai berikut :

1. Metode ini hanya mampu mendeteksi gambar yang dipalsukan dengan metode *copy move*.

2. Gambar bergerak seperti GIF tidak dapat diidentifikasi.
3. Metode ini hanya dapat menemukan gambar yang telah ditimpah, diduplikat (*cloning*), atau dimasukkan gambar lain (*splicing*).

#### **1.4. Tujuan Penelitian**

Tujuan penelitian ‘Identifikasi Gambar Digital Untuk Mengetahui Keaslian Gambar Dengan Metode *Inconsistent Shadow*’ ini adalah sebagai berikut :

1. Untuk membantu mendeteksi apakah gambar telah dimanipulasi atau tidak.
2. Mencari metode yang tidak memerlukan data mentah gambar.
3. Mencari metode yang tidak memerlukan *digital signature* atau *watermark* gambar untuk menentukan apakah gambar tersebut asli atau tidak.
4. Menentukan ketepatan akurasi metode *Inconsistent shadow*.

#### **1.5. Manfaat Penelitian**

Manfaat penelitian ‘Identifikasi Gambar Digital Untuk Mengetahui Keaslian Gambar Dengan Metode *Inconsistent Shadow*’ ini adalah sebagai berikut :

1. Menggabungkan metode *Inconsistent shadow* dan *algoritma robust* untuk mengidentifikasi pemalsuan gambar.
2. Membantu mendeteksi gambar yang dimanipulasi menggunakan gambar yang berada di media sosial.
3. Membantu menemukan objek apa saja yang dipalsukan dalam gambar.
4. Membantu mendeteksi pemalsuan gambar tanpa memerlukan data mentah dari gambar tersebut.

## II. TINJAUAN PUSTAKA

### 2.1. Pengolahan Citra Digital

Data atau informasi tidak hanya disajikan dalam bentuk teks. tapi dapat berupa gambar, audio (bunyi, suara, musik), dan video. Keempat macam data atau informasi tersebut sering disebut multimedia. Citra (*image*) istilah lain untuk gambar sebagai satu komponen multimedia memegang peranan penting sehingga bentuk informasi visual. Citra mempunyai karakteristik yang tidak dimiliki oleh data teks, yaitu citra kaya dengan informasi. Ada suatu peribahasa yang berbunyi “*a picture is more than a thousand words*” yang berarti suatu gambar akan lebih bermakna dari seribu kata. Maksudnya tentu suatu gambar dapat memberikan informasi yang lebih banyak dari pada informasi tersebut disajikan dalam bentuk kata-kata (tekstual).

Istilah citra atau gambar yang pada umumnya digunakan dalam bidang pengolahan citra diartikan sebagai suatu fungsi kontinu dari intensitas cahaya  $f(x,y)$  dalam bidang dua dimensi dengan  $(x,y)$  menyatukan suatu koordinat dengan nilai  $f$  pada setiap titik menyatukan intensitas atau tingkatan kecerahan atau derajat keabuan (*brightness / gray level*). Suatu citra digital adalah suatu citra kontinu yang diubah dalam bentuk diskrit, baik koordinat maupun intensitas cahayanya. Sehingga, dapat menganggap suatu citra digital sebagai suatu matriks,

dimana indeks baris dan kolomnya menyatakan koordinat sebuah titik pada citra tersebut dan nilai masing masing elemennya menyatakan intensitas cahaya pada titik tersebut.

Suatu titik pada sebuah citra digital sering disebut sebagai elemen citra (*image-elemen*), elemen gambar (*picture-elemen*), piksel (*pixel*). Pengolahan citra adalah pemrosesan citra, khususnya dengan menggunakan komputer menjadi citra yang kualitasnya lebih baik (Putra, 2010).

## **2.2. Foto Forensik**

Kemajuan terbaru dalam fotografi komputasi, visualisasi komputer, dan komputer grafis memungkinkan untuk menciptakan fotografi yang menarik secara palsu. Dimana menghasilkan penurunan kepercayaan pada foto dalam penegakan hukum, keamanan nasional, media, iklan, *e-commerce*, dan lainnya. Potensi dalam *image forensic* telah muncul untuk membantu mengembalikan beberapa kepercayaan dalam foto digital (Kee, *et al.*, 2013).

## **2.3. Digital Image Forensic**

*Digital Image Forensic* adalah bidang penelitian yang relatif baru tentang riwayat dari suatu gambar sedemikian rupa sehingga keasliannya dapat dievaluasi. *Image Forensic* didasarkan pada pengamatan bahwa proses pengolahan dilakukan tiap siklus gambar meninggalkan jejak tertentu, yang kehadirannya dapat dimanfaatkan untuk memaparkan manipulasi yang sesuai dengan jejaknya. Riwayat dari sebuah gambar dapat dibuktikan kebenarannya tanpa gambar aslinya, sebelum dimanipulasi (Sundaram and Nandini, 2014).

## **2.4. Resampling**

Untuk membuat gabungan dari beberapa gambar yang terlihat baik, sering dibutuhkan dengan mengubah ukuran, memutar, atau meregangkan bagian dari suatu gambar. Misalkan, saat membuat gabungan dari dua orang atau satu orang mungkin harus diubah ukurannya agar sesuai dengan ketinggian relatif. Proses ini membutuhkan *resampling* gambar asli ke sampel baru, mencocokkan korelasi periodik tertentu antara pixel satu dan pixel yang saling berhubungan. Karena korelasi ini tidak mungkin terjadi secara alami. Adanya resampling dapat digunakan untuk mendeteksi manipulasi tertentu (Farid, 2009).

## **2.5. Pemalsuan gambar**

Ada banyak jenis pemalsuan gambar yang paling umum dikategorikan menjadi tiga jenis yaitu :

### **2.5.1. Image Retouching**

*Image retouching* dapat dianggap sebagai pemalsuan digital yang tidak terlalu berbahaya. *Retouching* bukanlah apa apa melainkan menerapkan beberapa algoritma pengolahan citra gambar untuk meningkatkan atau mengurangi fitur tertentu dari suatu gambar. Tetapi tidak mengubah gambar secara signifikan. Hal ini dapat dikategorikan sebagai *soft forging*. Jenis pemalsuan ini pada umumnya digunakan oleh editor majalah untuk membuat gambar lebih menarik, tetapi pemalsuan gambar seperti ini masih salah secara moral (Sundaram and Nandini, 2014).

### **2.5.2. Splicing**

*Splicing* atau penyambungan juga disebut sebagai pemalsuan *Copy – Paste*. Hal ini dilakukan dengan mengambil daerah dari suatu gambar dan menempelkan ke target gambar lain, sehingga menghasilkan pemalsuan gambar. Hal ini sangat mungkin dalam metode ini memperlihatkan bahwa ketidakkonsistenan antara karakteristik gambar yang asli dan yang telah ditempelkan (Sundaram and Nandini, 2014).

### **2.5.3. Cloning**

Mungkin salah satu manipulasi gambar yang paling umum adalah *cloning (copy and move)* sebagian dari gambar untuk menyembunyikan seseorang atau objek dalam gambar. Bila hal ini dilakukan dengan hati hati, maka sulit untuk mendeteksi kloning secara visual, hal ini dikarenakan daerah kloning dapat menjadi bentuk apapun dan dimanapun, maka secara komputasi menjadi tidak mungkin untuk mencari semua lokasi dan ukuran gambar yang telah di *cloning* (Farid, 2009).

## **2.6. Bayangan**

Karakteristik bayangan menurut Yongzhen, *et al.* (2014) berisi banyak informasi dalam gambar digital. Ada banyak petunjuk visual penting dari bayangan seperti kedalaman, bentuk, isi, dan pencahayaan yang dideskripsikan sebagai berikut :

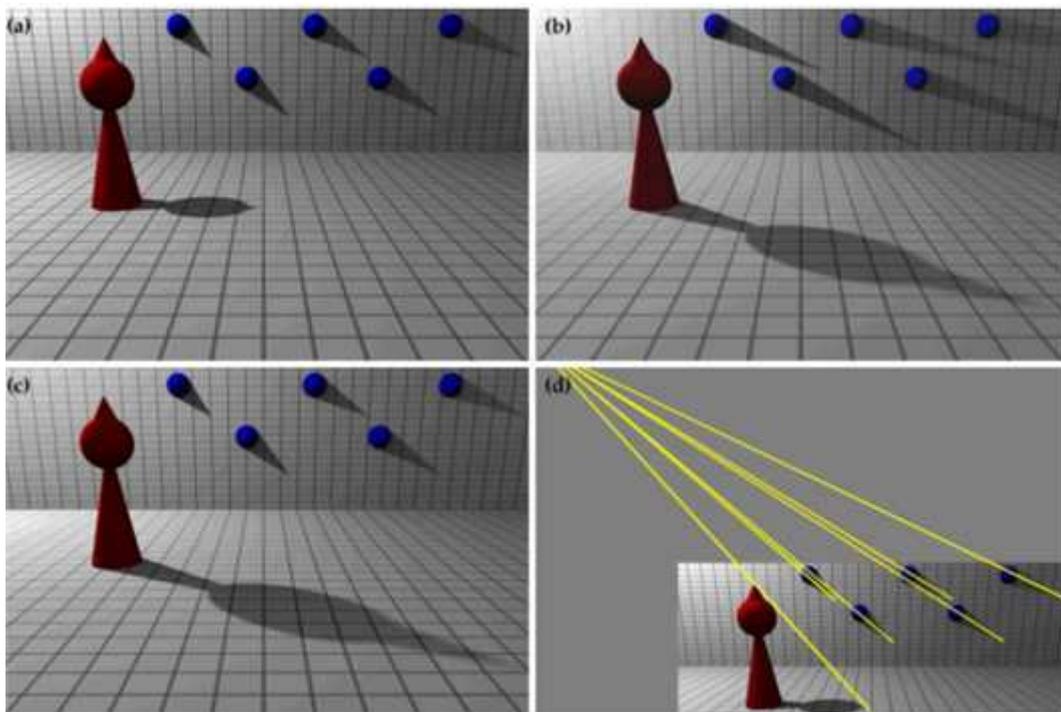
- a. Nilai piksel dari bayangan harus rendah dalam semua warna RGB.

Bayangan secara general lebih gelap dari daerah di sekitarnya.

- b. Bayangan tidak mengubah secara signifikan baik warna atau tekstur permukaan gambar yang ditutupi. Penutupan permukaan cenderung melanjutkan batas bayangan secara general.
- c. Bayangan selalu dikaitkan dengan objek yang membuatnya dan perilaku dari objek (contoh : jika seorang membuka lengannya, bayangan akan mencerminkan gerakan dan bentuk orang).
- d. Bentuk bayangan adalah proyeksi dari bentuk objek. Untuk sumber cahaya yang panjang (bukan titik sumber cahaya), proyeksi tidak mungkin perspektif.
- e. Posisi dan kekuatan dari sumber cahaya diketahui dari bayangan.
- f. Ukuran bayangan bergantung pada arah sumber cahaya dan ketinggian objek.

Gambar 2.4 (a) adalah adegan 3-D yang diterangi oleh cahaya tunggal yang menghasilkan bayangan pada permukaan dan dinding. Gambar (b) adalah gambar dengan adegan yang sama tetapi lokasi sumber cahaya dipindahkan sedikit. Gambar (c) adalah gabungan yang diciptakan dengan menggabungkan dinding dari gambar (a) dan permukaan dari gambar (b) untuk membuat adegan yang dengan bayang tidak konsisten dengan sumber cahaya tunggal. Untuk adegan dengan bayangan yang konsisnten, cahaya diposisikan baik di sisi kiri atau kanan ruangan dan di salah satu dari sembilan lokasi yang berbeda yang jaraknya bervariasi dari permukaan dan dari dinding. Untuk adengan dengan bayangan yang tidak konsisten, dinding dari adegan dengan pencahayaan berbeda dipertukarkan. Dua puluh orang diambil sebagai contoh untuk menduga apakah gambar adalah asli atau palsu dan diberikan waktu yang terbatas untuk menduga

gambar tersebut. Hasil pengujian hampir sempurna (95,5%) untuk menduga gambar palsu. Untuk semua kasus, ketepatan mengobservasi gambar adalah (52,8%). Rata – rata waktu yang dibutuhkan adalah 4.9 detik, menunjukkan bahwa pengamat menghabiskan waktu yang wajar dalam memeriksa tiap gambar. (Farid and Bravo, 2010).



**Gambar 1.** Bayangan yang terbentuk pada gambar

Pada bagian (a) dan (b) konsisten dengan cahaya tunggal. Bayangan pada gambar (c) adalah gabungan dari dinding gambar (a) dan permukaan gambar (b). Dalam hal ini =, bayangan yang terbentuk tidak konsisten terhadap cahaya tunggal. Garis kuning di gambar (d) menghubungkan titik –titik pada setiap objek ke arah bayangan yang dibentuk. Persimpangan garis –garis ini adalah lokasi 2-D dari cahaya.

## 2.7. Teknik Mendeteksi Pemalsuan Gambar

*Digital Image Foregery Detection Techniques* (DIFDT) merupakan klasifikasi kedalam pendekatan aktif dan pasif. Dalam pendekatan aktif, gambar digital memerlukan beberapa *preprocessing* seperti menanamkan *watermark* atau *signature generation* pada saat gambar diambil, hal ini didasarkan pada perhitungan *watermark* pada kamera. Kriptografi *digital signature* dan *digital watermark* yang digunakan sebagai sarana otentikasi gambar dalam banyak aplikasi. Kelemahan dari metode ini adalah bahwa *watermark* harus disisipkan pada saat gambar ditangkap. membatasi pendekatan ini hanya untuk kamera digital. Selain itu, ada jutaan gambar digital yang berada di internet tanpa *watermark* atau *digital signature*.

Oleh karena itu, dalam skenario seperti ini pendekatan aktif tidaklah layak untuk menemukan keaslian gambar. Berbeda dengan pendekatan aktif, teknik pasif digunakan tanpa memerlukan *watermark* atau *digital signature* yang tertanam dalam gambar. Teknik ini bekerja pada gagasan bahwa meskipun pemalsuan gambar digital mungkin tidak meninggalkan petunjuk visual yang menunjukkan pemalsuan, teknik ini dapat mengubah dasar statistik pada gambar (Sundaram and Nandini, 2014).

## 2.8. Teknik Mendeteksi Sumber Gambar

Menurut Sundaram dan Nandini (2014) sebuah gambar dapat berasal dari berbagai sumber pembuat gambar seperti kamera digital, komputer grafis, *scanner*, dll. Namun sumber pembuat gambar yang berbeda memiliki karakteristik yang berbeda, parameter yang berbeda diterapkan dan metode pengolahan gambar

diterapkan dalam perangkat. Jadi pola pola yang melekat dapat digunakan sebagai sidik jari untuk mengidentifikasi sumber gambar.

#### 1. Sumber forensik kamera digital

Dalam metode forensik gambar kamera digital, kepentingan utama adalah untuk menentukan sumber gambar dan mendeteksi *tampering*. Dalam metode yang ada, identifikasi sumber dicapai dengan menjelajahi berbagai tahap pengolahan di dalam kamera untuk memperoleh informasi yang membedakan dengan sumber kamera. Demikian pula inkonsistensi dalam kualitas gambar dianggap sebagai indikasi pemalsuan.

#### 2. *JPEG Quantization Table*

Umumnya kompresi JPEG digunakan untuk mengkodekan gambar dari kamera digital dan produsen yang berbeda biasanya mengkonfigurasi perangkat mereka dengan tingkat kompresi yang berbeda dan parameter. Dengan mengeksploitasi perbedaan ini dengan mengekstraksi tabel kuantisasi JPEG dari sebuah gambar dan membandingkannya dengan database kamera digital yang diketahui sumber indentifikasinya. Demikian juga, dapat dibandingkan dengan databse software *photo-editing* untuk tanda tanda pemalsuan.

Dari 204 kamera digital yang digunakan untuk percobaan, 62 kamera memiliki tabel kuantisasi unik sedangkan tabel yang tersisa jatuh ke kelas yang berkisar dari 2 hingga 28 dalam ukuran. Menggunakan lima versi dari *Adobe Photoshop*, suatu gambar (mungkin terkompresi) disimpan di masing – masing dari 13 tingkat kompresi dan ditemukan bahwa tabel

kuantitas JPEG digunakan berbeda dari 204 kamera tersebut. Jadi dengan mendeteksi keberadaan tabel kuantitas JPEG yang unik untuk setiap software *photo-editing* tertentu, dapat ditentukan jika gambar itu asli atau sebelumnya dirubah dan disimpan menggunakan software *photo-editing*.

### 3. *Chromatic Aberration*

Ada beberapa teknik dalam literatur yang diperkenalkan untuk mengevaluasi varians dari *Chromatic Aberration* untuk mengidentifikasi pemalsuan gambar. Teknik ini menggunakan sumber warna sebagai parameter keselarasan metrik berdasarkan informasi mutual juga diperhatikan. Kuantifikasi untuk meminimalkan kesalahan yang dilakukan antara atribut global dan lokal dengan mengevaluasi sudut *mean error*. Sebuah teknik berdasarkan *threshold* yang digunakan yaitu dimana jika *mean error* lebih dari ambang batas akan menunjukkan gambar yang bervariasi dalam gambar. Sehingga gambar yang tersebut berarti telah dirubah.

### 4. Pencahayaan

Teknik ini menggunakan identifikasi ragam dalam orientasi sumber cahaya yang berasal dari masing-masing objek dalam model dua dimensi. Teknik ini sangat tergantung pada sumber cahaya dan titik penerangan.

### 5. *Camera Response Function (CRF)*

Penggunaan *image splicing* juga terlihat pada teknik ini. Teknik ini menggunakan *invariants geometry* serta beberapa operasi tertentu dari perangkat penangkap gambar. Perbatasan *splicing* adalah *preliminarily*

(sebelumnya dan mengarah ke bagian utama) terdeteksi dan ekstraksi *invariants geometry* dilakukan dari piksel pada setiap bagian dari perbatasan menggunakan fungsi respon kamera tertentu. Perhitungan dilakukan untuk mengevaluasi konsistensi menggunakan teknik *cross-fitting*.

## **2.9. Anti Forensic**

*Anti-forensic* mampu mengelabui teknik forensik. Operasi anti forensik yang dirancang untuk menyembunyikan jejak dari manipulasi gambar dapat diterapkan ke gambar. Algoritma pendeteksi anti forensik adalah murni berdasarkan distribusi probabilitas koefisien. Dengan menambahkan beberapa jumlah *noise* yang disebut *anti-forensic dither* untuk gambar yang terkompresi sehingga distribusi yang ketat sesuai dengan yang diperkirakan. Distribusi gambar asli dan gambar yang diperkirakan adalah sama, sehingga teknik forensik gagal untuk menentukan modifikasi.

Operasi anti forensik meninggalkan sidik jari kompresi sendiri. Sebuah teknik baru telah diusulkan untuk mengetahui pengaruh anti forensik. Operasi pengolahan citra gambar anti forensik harus dikembangkan dan dipelajari sehingga kelemahan dalam teknik forensik gambar yang ada dapat diketahui oleh peneliti. Hal ini akan memungkinkan para peneliti untuk mengetahui kapan hasil forensik dapat dipercaya dan untuk membantu peneliti dalam mengembangkan teknik forensik digital. Studi tentang operasi anti-forensik juga dapat mengarah pada pengembangan teknik yang mampu mendeteksi ketika operasi anti forensik telah digunakan. (Abhita and Karthick, 2013).

## 2.10. *Confusion Matrix*

Menurut Prasetyo (2012) sebuah sistem yang melakukan klasifikasi diharapkan dapat melakukan klasifikasi semua set data dengan benar, tetapi tidak dapat dipungkiri bahwa kinerja suatu sistem tidak bisa 100% benar sehingga sebuah sistem klasifikasi juga harus diukur kinerjanya. Umumnya, pengukuran kinerja klasifikasi dilakukan dengan matriks konfusi (*confusion matrix*).

Matriks konfusi merupakan tabel pencatat hasil kerja klasifikasi. Kuantitas matriks konfusi dapat dibagi menjadi dua nilai, yaitu akurasi dan laju *error*. Dengan mengetahui jumlah data yang diklasifikasikan secara benar, kita dapat mengetahui akurasi hasil prediksi dan dengan mengetahui jumlah data yang diklasifikasikan secara salah, dapat mengetahui laju *error* dari prediksi yang dilakukan. Dua kuantitas ini digunakan sebagai matrik kinerja klasifikasi. Untuk menghitung akurasi digunakan formula.

$$\text{Akurasi} = \frac{\text{jumlah data yang diprediksi secara benar}}{\text{jumlah prediksi yang dilakukan}} = \frac{f_{11} + f_{00}}{f_{11} + f_{10} + f_{01} + f_{00}} \quad (1)$$

Untuk menghitung laju *error* (kesalahan prediksi) digunakan formula.

$$\text{Error} = \frac{\text{jumlah data yang diprediksi secara salah}}{\text{jumlah prediksi yang dilakukan}} = \frac{f_{10} + f_{01}}{f_{11} + f_{10} + f_{01} + f_{00}} \quad (2)$$

Semua algoritma klasifikasi berusaha membentuk model yang mempunyai akurasi tinggi atau (laju *error* yang rendah). Umumnya, model yang dibangun memprediksi dengan benar pada semua data yang menjadi data latihnya, tetapi ketika model berhadapan dengan data uji, barulah kinerja model dari sebuah algoritma klasifikasi ditentukan.

### 2.11. *Robust Algorithm*

pengujian menggunakan algoritma robust detection mengidentifikasi bagian gambar yang sama persis. Tahap pertama adalah menentukan besaran resolusi gambar, misal  $B \times B$  pixel. Kemudian gambar dipindai dari pojok kiri atas menuju pojok kanan bawah sambil menentukan blok  $B \times B$ . Untuk tiap blok koefisien akan disimpan di matriks A. Matriks tersebut memiliki  $(M - B + 1)(N - B + 1)$  kolom dan  $B \times B$  baris untuk tiap gambar yg sama ketika terdeteksi. (Popescu, 2004)

Ketika ada dua baris matriks A yg diurutkan telah didapatkan, algoritma akan menyimpan posisi blok yg teridentifikasi sama di daftar yang berbeda (contoh, koordinat dibagian kiri atas pixel dari suatu blok dapan diambil sebagai posisinya) dan menambahkan sebuah koter pergeseran vektor C. Asumsikan  $(i_1, i_2)$  dan  $(j_1, j_2)$  sebagai posisi dari kedua blok yang kembar. Pergeseran vektor s antara kedua blok yang kembar dihitung :

$$s=(s_1, s_2)=(i_1-i_2, j_1-j_2). \quad (3)$$

Karena pergeseran vektor  $-s$  dan  $s$  memiliki pergeseran yang sama, pergeseran vektor dapat dinormalisasikan bila perlu, dengan mengkalikannya dengan  $-1$  sehingga  $s_1 \geq 0$ . Untuk tiap blok, dengan menambahkan vektor yang dinormalisasikan dengan satu :

$$C(s_1, s_2)= C(s_1, s_2)+1. \quad (4)$$

Pergeseran vektor C diinisialisasikan dengan nol sebelum algoritma dimulai. Pada akhir proses pencocokan, pencacah C menunjukkan frekuensi dimana terjadi pergeseran vektor dinormalisasi yang berbeda. (Fridrich, 2003).

### **III. METODE PENELITIAN**

#### **3.1. Waktu dan Tempat**

Penelitian ini dilakukan di lingkungan jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung. Waktu penelitian dilaksanakan pada semester 7 tahun ajaran 2016/2017.

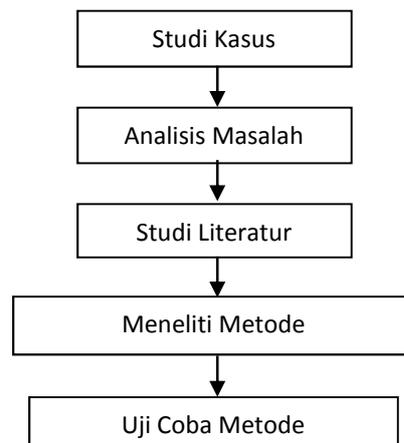
#### **3.2. Alat dan Bahan**

Alat dan bahan yang digunakan untuk mendukung penelitian ini dapat diperoleh dari mengidentifikasi dan mengumpulkan studi literatur mengenai perangkat keras dan perangkat lunak yang digunakan dalam penelitian ini. Dalam penelitian ini penulis menggunakan perangkat keras (*hardware*) dan perangkat lunak (*software*) sebagai berikut.

- a. Perangkat notebook dengan spesifikasi sebagai berikut :
  - *Processor* : Intel Celeron 1,5GHz
  - *RAM* : DDR3 4 GB
  - *Hardisk* : 500 GB
  - *Display* : Intel HD Graphics
- b. Perangkat lunak (*software*) yang digunakan :
  - Sistem Operasi : Windows 7 64 Bit.
  - Aplikasi : Adobe Photoshop, Anaconda (Python), Library PIL

### 3.3. Tahap Penelitian

Penelitian ini bertujuan untuk menemukan kejanggalan pada sebuah foto melalui bayangan dengan menentukan apakah foto tersebut masih asli atau telah dimanipulasi. Dengan menggunakan metode *Inconsistent shadows*. Metode tersebut diaplikasikan ke dalam sebuah kode sederhana menggunakan bahasa pemrograman *Python*. Dengan meneliti bayangan dari objek dapat ditentukan objek mana yang kemungkinan telah ditambahkan kedalam sebuah gambar, seperti duplikasi suatu objek (*cloning*) atau menutupi suatu gambar dengan gambar lainnya (*splicing*). Flowchart tahapan penelitian yang menjelaskan proses penelitian ini ditunjukkan pada Gambar 3.1.



**Gambar 2.** *Flowchart* alur metodologi penelitian

#### a. Studi Kasus

Pada tahap ini peneliti menyelidiki suatu gejala pemalsuan data dalam beberapa kasus, seperti pada kasus penyebaran informasi menggunakan media gambar palsu, kasus hukum yang sedang diinvestigasi

menggunakan media gambar sebagai barang bukti, dan kasus pemalsuan gambar lainnya.

#### b. Analisis Masalah

Pada tahap ini setelah peneliti mempelajari beberapa kasus, peneliti merencanakan suatu metode untuk memudahkan para penyidik untuk menemukan kejanggalan kejanggalan pada suatu gambar yang ada. Dengan mudahnya informasi yang menyebar, canggihnya teknologi untuk memanipulasi data dan besarnya pemalsuan data pada saat ini, maka pemilihan suatu metode sangat menentukan untuk menyelidiki apakah gambar telah dimanipulasi atau tidak.

#### c. Studi Literatur

Pada tahap ini penulis mempelajari dan mengumpulkan data yang dibutuhkan untuk penelitian dengan literatur literatur seperti buku dan jurnal yang ada hubungannya dengan penelitian yang dilakukan.

#### d. Meneliti Metode.

Pada tahap ini metode dikembangkan dengan menggunakan informasi yang didapat dari bayangan yaitu :

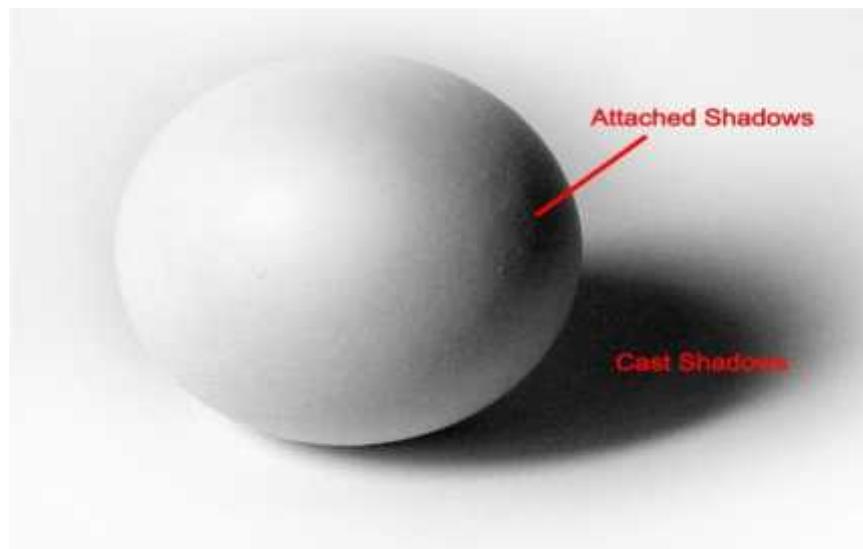
##### 1. *Cast Shadows* (Kee, et al., 2013).

*Cast shadows* adalah bayangan yang diciptakan dari sebuah objek, pada Gambar 1 Dimana dijelaskan bahwa bayangan yang terletak di belakang suatu objek disebut *cast shadows*. *Cast shadows* dapat dijadikan sebuah *constraint* dalam menentukan pemalsuan gambar

dengan menentukan arah bayangan yang tercipta dari suatu objek. Lokasi proyeksi dari sumber cahaya harus bersimpangan (persimpangan dapat terjadi meskipun di luar dari batas gambar dengan memperpanjang garis sehingga garis dapat bersimpangan).

## 2. *Attached Shadows* (Kee, et al., 2013).

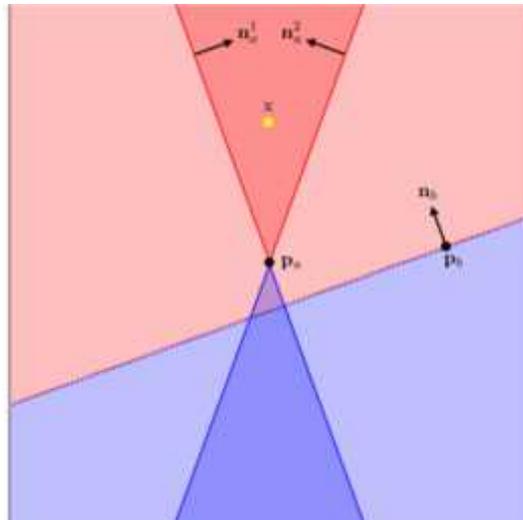
*Attached Shadows* adalah bayangan yang menutupi sebagian permukaan dari objek. Pada Gambar 1 dijelaskan posisi *attached shadows*. *Attached shadows* terjadi ketika benda menutupi jalan cahaya dari objek itu sendiri, meninggalkan sebagian dari objek dalam bayangan.



**Gambar 3.** *Cast and Attached Shadow*

Dapat dilihat gambar suatu bola dengan bayangannya. *Cast shadows* adalah bayangan yang terletak di belakang dari suatu objek, bayangan ini harus memiliki proyeksi yang sejajar untuk menunjukkan bahwa bayangan tersebut sesuai dengan objeknya. *Attached shadows* adalah bayangan yang menutupi sebagian permukaan objek, *attached*

*shadows* terletak dibagian belakang dari objek yang menghadap lurus ke arah cahaya.



**Gambar 4.** Gambar irisan *constraint*

Irisan *constraint* didefinisikan oleh dua garis (merah tua) dan *constraint* setengah bagian permukaan didefinisikan sebagai satu garis (merah putus putus). Lokasi proyeksi dari sumber cahaya (titik kuning,  $x$ ) terletak didalam wilayah (garis hitam) yang terbentuk oleh persimpangan antar *constraint*, bagian biru adalah inversi dari *constraint*.

### 3. Forensik menggunakan bayangan

Untuk menentukan keaslian gambar menggunakan bayangan, harus ada lokasi permukaan infinit ( $\mathbb{R}^2$ ) yang memenuhi semua *constraint* dari *cast shadows* dan *attached shadows*. Artinya persimpangan dari semua *constraint* harus mendefinisikan wilayah yang tidak kosong.

*Cast* dan *attached shadows constraint* dapat direpresentasikan sebagai pertidaksamaan linear. Ketepatan dari *constraint* ini dapat ditentukan

dengan menggunakan pemrograman linear standar. Pada Gambar 2 terdapat dua garis yang didefinisikan secara implisit oleh normal  $n_\alpha^1$  dan  $n_\alpha^2$  dan titik  $p_\alpha$ . Arah normal menunjukkan wilayah pada permukaan  $x$  bertempat seharusnya. persimpangan antara dua wilayah ini adalah daerah segitiga berwarna merah. Pada Gambar 3 juga terdapat garis tunggal didefinisikan oleh normal  $n_b$  dan titik  $p_b$ . Garis ini menetapkan setengah permukaan *constraint* dimana target seharusnya berada. Pada tiap kasus, *constraint* bayangan ditetapkan oleh sepasang garis yang membentuk segitiga (*constrained wedge cast shadows*) atau garis tunggal (*constrained half plane attached shadows*).

Secara umum, *constraint half plane* ditetapkan dengan pertidaksamaan linear tunggal pada  $x$  yang tidak diketahui :

$$n_i \cdot x - n_i \cdot p_i \geq 0, \quad (3)$$

dengan  $n_i$  adalah baris normal dan  $p_i$  adalah titik pada garis. Sebuah *constrained* berbentuk segitiga ditetapkan dengan dua linear *constraint* :

$$n_i^1 \cdot x - n_i^1 \cdot p_i \geq 0 \text{ dan } n_i^2 \cdot x - n_i^2 \cdot p_i \geq 0. \quad (4)$$

Sekumpulan dari *constraint half plane* dan *wedge* dapat dikombinasikan menjadi suatu sistem dari pertidaksamaan  $m$  :

$$\begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_m \end{pmatrix} x - \begin{pmatrix} n_1 \cdot p_1 \\ n_1 \cdot p_1 \\ \vdots \\ n_1 \cdot p_1 \end{pmatrix} \geq 0, \quad (5)$$

$$Nx - P \geq 0. \quad (6)$$

Mengingat *constraint* yang tidak *error* pada kasus yang konsisten, solusi pada sistem pertidaksamaan harus ada. Untuk menjelaskan kesalahan atau inkonsistensi dapat menggunakan suatu set *m surplus variable*  $s_i$  :

$$Nx - P = -s. \quad (7)$$

$$S \geq 0. \quad (8)$$

Dengan  $s_i$  adalah komponen ke  $i^{\text{th}}$  dari  $m$ -vektor  $s$ . Jika *constraint* telah terpenuhi maka solusi akan muncul ketika semua *surplus variable* bernilai nol. Solusi dengan *surplus variable*  $s_i$  yang tidak bernilai nol berarti solusi tersebut tidak konsisten dengan *constraint*  $i$ . Rumus pertidaksamaan dapat dikombinasikan kedalam suatu sistem sebagai berikut :

$$\begin{pmatrix} N & I \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ s \end{pmatrix} - \begin{pmatrix} P \\ 0 \end{pmatrix} \geq 0. \quad (9)$$

dengan  $I$  adalah matriks identitas  $m \times m$ . Dengan demikian program linear tersebut meminimalkan  $L_i$  normal dari vektor *surplus variable*.

$$(0 \ 1) \begin{pmatrix} x \\ s \end{pmatrix}. \quad (10)$$

yang didapat dari *constraint* pada Persamaan (9). Artinya, untuk menentukan solusi yang meminimalkan *surplus variable*, cukup dipenuhi semua *constraint cast shadow* dan *attached shadow*. Jika *surplus variable* untuk solusi optimal adalah nol, maka ada posisi cahaya yang memenuhi semua *constraint* yang telah ditetapkan. Jika tidak, satu atau lebih dari bayangan tidak konsisten dengan sisa dari kasus.

Perlu diingat bahwa *constraint* bayangan ditetapkan dengan menghubungkan titik pada bayangan dengan berbagai titik kemungkinan yang sesuai pada objek. Ada tanda ambiguitas yang melekat dalam menentukan *constraint* : jika cahaya berada di belakang pusat proyeksi, maka lokasi yang diproyeksikan pada bidang gambar terbalik dan semua *constraint* harus diabaikan. Dalam kasus ini, *constraint* mengambil bentuk :

$$-Nx + P -s. \quad (11)$$

Pada Gambar 3 dapat diambil contoh daerah biru yang menghadap kebawah adalah inversi yang sesuai dengan daerah merah yang menghadap ke atas. Untuk menyelesaikan masalah ini dapat menggunakan persamaan (7) dan (11) dan memilih solusi dengan minimal  $L_1$ , pada persamaan (10) jika sistem biasa atau yang terinversi memiliki solusi dengan *surplus* nol, maka dapat disimpulkan bahwa *constraint* konsisten. Jika tidak, tidak ada posisi cahaya yang konsisten dengan semua *constraint* dan dapat disimpulkan bahwa beberapa *constraint* yang dihasilkan oleh bagian gambar telah dimanipulasi.

Ketika gambar menghasilkan *constraint* yang inkonsisten, untuk dapat mengetahui *constraint* bagian mana yang menyebabkan inkonsistensi. *Constraint* yang saling bertentangan memberikan bukti penting yang dapat digunakan untuk menentukan pemalsuan gambar, dan dapat berguna dalam menentukan dalam menentukan bagian mana pada gambar yang telah dimanipulasi. Untuk memulai, dua *constraint*

dipilih secara acak. Jika *constraint* ini tidak memenuhi, maka *constraint* tersebut akan membentuk satu set minimal *constraint* inkonsisten. Jika memenuhi, maka *constraint* yang dipilih secara acak ditambahkan ke set dan program linear diselesaikan. *Constraint* ditambahkan dengan cara ini sampai sistem tidak lagi memenuhi persyaratan. Seluruh proses ini diulang dengan kondisi awal secara acak yang berbeda. set *constraint* terkecil yang bertentangan, mungkin atau tidak bersifat unik, memberikan ringkasan singkat dari bagian gambar yang mana yang telah diubah.

#### 4. *Robust Algorithm*

Menurut (Popescu, 2004) pengujian menggunakan algoritma *robust detection* mengidentifikasi bagian gambar yang sama persis. Tahap pertama adalah menentukan besaran resolusi gambar, misal  $B \times B$  pixel. Kemudian gambar dipindai dari pojok kiri atas menuju pojok kanan bawah sambil menentukan blok  $B \times B$ . Untuk tiap blok koefisien akan disimpan di matriks  $A$ . Matriks tersebut memiliki  $(M - B + 1)(N - B + 1)$  kolom dan  $B \times B$  baris untuk tiap gambar yg sama ketika terdeteksi.

Menurut (Fridrich, 2003) Ketika ada dua baris matriks  $A$  yg diurutkan telah didapatkan, algoritma akan menyimpan posisi blok yg teridentifikasi sama di daftar yang berbeda (contoh, koordinat di bagian kiri atas pixel dari suatu blok dapan diambil sebagai posisinya) dan menambahkan sebuah koter pergeseran vektor  $C$ .

Asumsikan  $(i_1, i_2)$  dan  $(j_1, j_2)$  sebagai posisi dari kedua blok yang kembar. Pergeseran vektor  $s$  antara kedua blok yang kembar dihitung :

$$s = (s_1, s_2) = (i_1 - i_2, j_1 - j_2). \quad (12)$$

Karena pergeseran vektor  $-s$  dan  $s$  memiliki pergeseran yang sama, pergeseran vektor dapat dinormalisasikan bila perlu, dengan mengkalikannya dengan  $-1$  sehingga  $s_1 \geq 0$ . Untuk tiap blok, dengan menambahkan vektor yang dinormalisasikan dengan satu :

$$C(s_1, s_2) = C(s_1, s_2) + 1. \quad (13)$$

Pergeseran vektor  $C$  diinisialisasikan dengan nol sebelum algoritma dimulai. Pada akhir proses pencocokan, pencacah  $C$  menunjukkan frekuensi dimana terjadi pergeseran vektor dinormalisasi yang berbeda

#### e. Uji coba metode

Pada tahap ini peneliti akan mengujikan metode *Inconsistent shadows* dengan menggunakan program sederhana yang dibuat menggunakan bahasa pemrograman *python* untuk menentukan hasil dari metode yang dikembangkan dengan mengujikan program untuk mengidentifikasi beberapa gambar. Dengan mengujikan 35 gambar yang diambil secara acak dari internet kemudian dilakukan modifikasi terhadap gambar, peneliti akan melakukan pengujian menggunakan algoritma *robust detection* yg berfokuskan pada pengujian pixel yang ada di gambar. Jika gambar berhasil dideteksi setelah diedit maka persentasi kebenarannya dapat dihitung.

Sebuah sistem yang melakukan klasifikasi diharapkan dapat melakukan klasifikasi semua set data dengan benar, tetapi tidak dapat dipungkiri bahwa kinerja suatu sistem tidak bisa 100% benar sehingga sebuah sistem klasifikasi juga harus diukur kinerjanya. Umumnya, pengukuran kinerja klasifikasi dilakukan dengan *confusion matrix* (Prasetyo, 2012). Dengan menggunakan *confusion matrix* maka dapat diukur akurasi klasifikasi gambar yang akan diujikan.

*Confusion matrix* merupakan tabel pencatat hasil kerja klasifikasi. Dengan mengetahui jumlah data yang diklasifikasikan secara benar, maka akan diketahui akurasi hasil prediksi dan dengan mengetahui jumlah data yang diklasifikasikan secara salah, maka akan diketahui laju *error* dari prediksi yang dilakukan. Dua kuantitas ini digunakan sebagai matrik kinerja klasifikasi. Untuk menghitung akurasi digunakan formula.

$$\text{Akurasi} = \frac{\text{jumlah data yang diprediksi secara benar}}{\text{jumlah prediksi yang dilakukan}} = \frac{f_{11}+f_{00}}{f_{11}+f_{10}+f_{01}+f_{00}} \quad (14)$$

Untuk menghitung laju *error* (kesalahan prediksi) digunakan formula.

$$\text{Error} = \frac{\text{jumlah data yang diprediksi secara salah}}{\text{jumlah prediksi yang dilakukan}} = \frac{f_{10}+f_{01}}{f_{11}+f_{10}+f_{01}+f_{00}} \quad (15)$$

Uji coba akan menentukan seberapa besar ketepatan algoritma dapat menentukan apakah gambar tersebut masih asli atau sudah diubah. Karena metode ini masih memerlukan perspektif manusia dalam menentukan *constraint* maka akan sangat mungkin terjadi perbedaan perspektif dalam menentukan *constraint* yang mana yang harus diuji dalam gambar untuk dapat menentukan apakah gambar tersebut masih asli atau tidak.

## V. KESIMPULAN

### 5.1. Kesimpulan

Kesimpulan dalam penelitian ini adalah sebagai berikut :

1. Metode *Inconsistent shadow* yang diuji menggunakan algoritma Robust dapat mendeteksi gambar yg telah dimanipulasi dengan teknik *splicing* dan *cloning* dengan akurasi sebesar 91,42 %.
2. Metode *Inconsistent shadow* yang diuji menggunakan algoritma Robust tidak memerlukan data mentah gambar karena metode *Inconsistent shadow* menggunakan bayangan dalam mendeteksi gambar sedangkan algoritma Robust menggunakan pengelompokan piksel dalam mendeteksi gambar.
3. Metode *Inconsistent shadow* yang diuji menggunakan algoritma Robust tidak memerlukan *digital signature* atau *watermark* karena metode *Inconsistent shadow* menggunakan bayangan dalam mendeteksi gambar sedangkan algoritma Robust menggunakan pengelompokan piksel dalam mendeteksi gambar.
4. Ketepatan akurasi dari metode *Inconsistent shadow* yang telah diujikan menggunakan algoritma Robust menunjukkan bahwa algoritma Robust lebih baik jika metode *Inconsistent shadow* menggunakan 10 dan 20 konstrain dengan akurasi 91% berbanding dengan 80% sedangkan metode

*Inconsistent shadow* lebih baik dibanding dengan algoritma Robust jika menggunakan 50 konstrain dengan akurasi 91% berbanding dengan 100%.

## 5.2. Saran

1. Mencari metode yang lebih cepat dan efisien dalam masalah waktu.
2. Memperbanyak dataset dan membandingkannya dengan penelitian yang lain.
3. Mengimplementasikan metode *Inconsistent shadow* ke dalam program secara otomatis agar tidak diperlukan manusia untuk menentukan konstrain secara manual.

## DAFTAR PUSTAKA

- Abhitha. E., Karthick.A. 2013. Forensic Technique for Detecting Tamper in Digital Image Compression. *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 2, Issue 3, pr 1325-1330.
- Farid, H. 2009. A Survey of Image Forgery Detection. *IEEE Signal Processing Magazine*. Vol. 26, Issue 2, pp 16-25.
- Farid, H. and Bravo, M. J. 2010. Image forensic analyses that elude the human visual system. *In SPIE Conference on Media Forensics and Security*. Vol. 7541, p. 754106 - 754123.
- Fridrich, A. Jessica, B. David Soukal, and A. Jan Lukáš. 2003. Detection of copy-move forgery in digital images. *Proceedings of Digital Forensic Research Workshop*.
- Kee, E., O'Brien, J. F., and Farid, H., 2013. Exposing Photo Manipulation with Inconsistent Shadows. *ACM Trans. Graph*. Vol. 32, Issue 4, 1-12.
- Prasetyo, Eko. 2012. Data Mining Konsep dan Aplikasi Menggunakan MATLAB. Yogyakarta, Andi.
- Putra, Darma. 2010. *Pengolahan Citra Digital*. Yogyakarta, Andi.
- Popescu. A.C. and H. Farid. 2004. Exposing Digital Forgeries by Detecting Duplicated Image Regions. *TR2004-515, Department of Computer Science, Dartmouth College*.
- Sundaram, A. M., and Nandini, C., 2014. Investigational Study of Image Forensic Applications, Techniques and Research Directions. *International Journal of Emerging Technology and Advanced Engineering*. Vol. 4, Issue 8, 1-9.
- Yongzhen Ke, Fan Qin, Weidong Min, and Guiling Zhang. 2014. Exposing Image Forgery by Detecting Consistency of Shadow. *The Scientific World Journal*. pp 1-9.