# A Review Paper: Image Manipulation Passive Detection in Digital Image Processing

Sjahrul Haitami[1], Setyawan Widyarto[2]

[1]Universitas Budi Luhur
1811600954@student.budiluhur.ac.id
[1, 2]Centre for Graduate Studies (CGS), Universiti Selangor
swidyarto@gmail.com

## Abstract:

The use of images in electronic communication is widely used today, it is said that images can convey messages more clearly than thousands of words. But the image can be manipulated so that it gives the wrong message and it can cause chaos. For this reason, a method is required to confirm that the image received is in its original condition and has not been manipulated. There are two classifications in image manipulation detection, the first is active detection that is the authenticity of the image is determined by the information embedded in the image such as a digital signature or watermarking. The second is passive detection where the originality of the image is determined without prior knowledge embedded in the image so that the detection is through manipulation operations performed on the image or through identification of the source image. Active detection will certainly give the best results, but because many images do not have embedded data requirements beforehand, the use of passive detection methods increases in popularity. This paper will review the passive detection method, spesifically by tampering operation used in digital image processing on detecting manipulated images and comparing them.

**Purpose:** This paper will reveil method use in digital image processing in pasif detection of manipulated image and find the best method available.
**Background:** The use of an image in electronic communication is growing but digital image can be manipulated easily thus can make people mislead.
**Design/Methodology/Approach:** This paper will review techniques use in pasif detection of manipulated image base on image tampering operation.
**Results/Findings:** There is many type of image manipulation techniques and each needs specific way to detect.
**Conclusion and Implications:** To increase detection of image manipulation it needs to use more than one method and combine them.

**Keywords**: active detection, image manipulation, passive detection, tempering operation

## ABSTRAK

Penggunaan gambar dalam komunikasi elektronik banyak digunakan saat ini, konon gambar dapat menyampaikan pesan lebih jelas dari ribuan kata. Tetapi gambar dapat dimanipulasi sehingga memberikan pesan yang salah dan hal tersebut dapat mengakibatkan kekacauan. Untuk itu diperlukan metode untuk mengkonfirmasi bahwa gambar yang diterima dalam kondisi asli dan belum dimanipulasi. Ada dua klasifikasi dalam deteksi manipulasi gambar, yang pertama adalah deteksi aktif yaitu keaslian gambar ditentukan oleh informasi yang tertanam dalam gambar seperti tanda tangan digital atau *watermarking*. Yang kedua adalah pendeteksian pasif dimana orisinalitas gambar ditentukan tanpa adanya pengetahuan sebelumnya yang tertanam didalam gambar sehingga deteksinya melalui operasi manipulasi yang dilakukan terhadap gambar ataupun melalui identifikasi sumber gambar. Deteksi aktif tentu akan memberikan hasil terbaik, tetapi karena banyak gambar tidak memiliki persyaratan data tertanam sebelumnya maka penggunaan metode deteksi pasif meningkat popularitasnya. Makalah ini akan meninjau metode deteksi pasif, khususnya dalam *tampering operation* yang digunakan dalam pemrosesan gambar digital untuk mendeteksi gambar yang dimanipulasi dan membandingkannya.


**Kata Kunci**: deteksi aktif, deteksi pasif, manipulasi gambar, *tampering operation*

## 1. PENDAHULUAN

Salah satu peribahasa terkenal mengatakan "Sebuah gambar bernilai seribu kata" dan banyak orang mengerti maksud dari peribahasa tersebut. Tetapi karena perkembangan tehnologi memungkinkan untuk manipulasi gambar dengan sangat mudah sehingga siapa pun dengan sedikit keterampilan computer dapat melakukannya. Oleh karena itu peribahasa di atas dapat kehilangan esensinya karena pesan yang salah diterima akibat gambar manipulasi [1]. Perubahan gambar dalam perspektif karya digital dapat dianggap sebagai karya kreatif, akan tetapi dalam beberapa kasus gambar yang diubah disalahgunakan dengan maksud jahat. Kondisi seperti itu seringkali muncul ketika gambar menjadi bukti hukum, seperti untuk laporan medis pada tempat kejadian kejahatan dimana gambar penyebab kematian pasien dipalsukan dan penjahatnya melarikan diri. Contoh lainnya adalah dalam penelitian ilmiah, pemilik data sangat berhati-hati dalam menerbitkan gambar mereka tanpa kepemilikan dan hak cipta sehingga mengurangi ketersediaan data untuk para peneliti lainnya. Demikian juga banyak masalah lainhnya muncul dibidang yang berbeda karena perubahan atau manipulasi gambar. Oleh karena hal tersebut diatas maka diperlukan suatu teknik untuk dapat mendeteksi manipulasi image sehingga akibat buruk karena gambar termanipulasi dapat dicegah.

## 2. TINJAUAN PUSTAKA

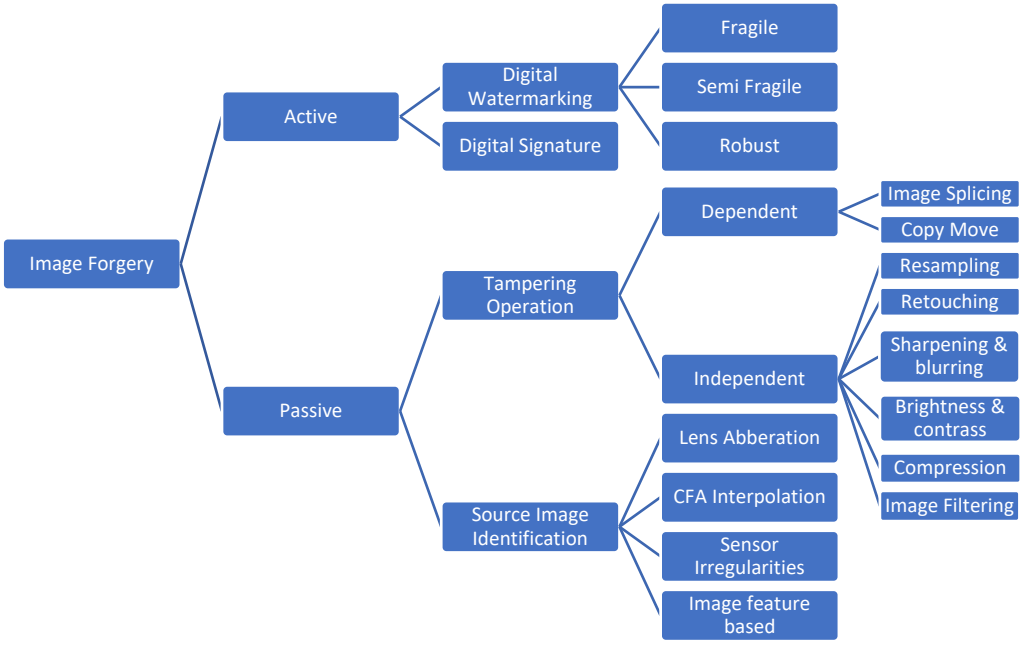
Teknik deteksi pemalsuan gambar diklasifikasikan menjadi dua pendekatan yang berpusat pada persyaratan pengetahuan sebelumnya untuk deteksi pemalsuan. Mereka adalah deteksi pemalsuan berdasarkan pendekatan aktif yaitu dengan tanda tertentu yang disimpan dalam image, baik terlihat maupun tersembunyi dan pendekatan pasif yaitu dengan meneliti gambar berdasarkan operasi manipulasi yang telah dilakukan ataupun identifikasi sumber gambar tersebut [2].

Deteksi pemalsuan aktif atau *nonblind* adalah metode tradisional yang digunakan untuk mendeteksi manipulasi gambar berdasarkan beberapa informasi sebelumnya tentang gambar yang mungkin telah tertanam dalam gambar pada saat pengambilan gambar atau selama akuisisi gambar atau tahap selanjutnya. Contoh dari deteksi pemalsuan gambar aktif adalah melalui *digital watermarking* dan *digital signature* yang terdapat didalam gambar. Pendekatan aktif memverifikasi keaslian gambar dengan cara menyembunyikan skema. Tanda air atau tanda tangan digital adalah data yang disembunyikan di dalam gambar pada saat pembuatan. Pada saat pemeriksaan keaslian di pihak penerima, data atau tanda rahasia dipulihkan dan diverifikasi dengan data yang disimpan pada proses pembuatan.

Deteksian pemalsuan pasif sangat berbeda dengan pendekatan aktif, pada pendekatan pasif manipulasi gambar dideteksi tanpa pengetahuan sebelumnya dalam gambar asli

atau fitur-fiturnya. Untuk memverifikasi keaslian gambar, statistik dan konten gambar yang tersedia digunakan dalam pendekatan pasif. Proses verifikasi dilakukan berdasarkan informasi penggabungan gambar itu sendiri tanpa menggunakan informasi tambahan apa pun. Karena pendekatan pasif mengotentikasi gambar palsu berdasarkan pengetahuan yang tersedia, itu juga disebut sebagai pendekatan buta atau *blind*. Tipe dari deteksi pemalsuan gambar pasif dibagi menjadi dua bagian yaitu berdasarkan teknik manipulasi imagenya dan berdasarkan identifikasi sumber gambarnya.

Secara singkat klasifikasi deteksi manipulasi image dapat dibuat menjadi diagram sederhana seperti gambar dibawah.




Gambar 1. Klasifikasi deteksi manipulasi gambar

Metode deteksi aktif menggunakan data atau informasi tertanam dalam gambar akan memberikan hasil keaslian paling baik karena gambar dapat dengan mudah diverivikasi berdasarkan informasi tersebut, tetapi digital image yang banyak beredar tidak memiliki persyaratan seperti itu sehingga dibutuhkan metode deteksi pasif yang mampu menguji keaslian gambar menggunakan informasi gambar yang ada saja. Untuk itu dalam makalah ini dikhususkan mencari pengetahuan dalam literature yang melakukan deteksi image palsu secara pasif berdasarkan operasi manipulasi yang dilakukan atau *tampering operation*.

*Image tampering operation* adalah berarti manipulasi atau perubahan pada gambar untuk mengubah makna semantiknya untuk tujuan ilegal atau tidak sah. Bagian ini dibagi dua menjadi *dependent* dan *independent*. Maksud dari *dependent* adalah manipulasi dapat dilakukan dalam gambar yang sama dengan menyalin dan menempel beberapa area di dalam gambar atau lebih dari satu gambar dapat digabungkan untuk mendapatkan komposit yang meyakinkan, terdiri dari *image splicing* dan *copy-move*. Sedangkan maksud dari *independent* adalah pemalsuan independen diantaranya *resampling*, *retouching*, rotasi gambar, penskalaan, pengubahan ukuran, penambahan noise, pengkaburan dan pengkompresian gambar. Jadi dalam *independent tampering operation image* yang dimanipulasi adalah dirinya sendiri atau independent tanpa gabungan dari image lainnya.

## 3. METODOLOGI PENELITIAN

Untuk melakukan penelitian pada makalah ini maka digunakan langkah-langkah dibawah:

1) Melakukan studi pustaka mengenai pengolahan citra digital untuk deteksi pemalsuan gambar.

2) Mencari paper yang telah melakukan penelitian tentang deteksi pemalsuan gambar.
3) Melakukan analisis pembandingan metode dan evaluasi hasil dari penelitian pada paper yang dikumpulkan.
4) Membuat kesimpulan beserta saran dari paper yang telah dibandingkan.

## 4. HASIL DAN PEMBAHASAN

Setelah dilakukan studi literatur mengenai penelitian untuk mendeteksi manipulasi gambar dengan algoritma tertentu maka disajikan 10 literatur dan didapatkan data-data yang dirangkum dalam tabel dibawah ini.

Tabel 1. Ringkasan literatur

| No | Judul, tahun | Manipulasi | Metode | Hasil |
|---|---|---|---|---|
| 1 | Fighting Fake News: Image Splice Detection via Learned Self-Consistency, 2018 [3] | Image Splicing | Algoritma pembelajaran untuk mendeteksi manipulasi gambar visual yang dilatih menggunakan dataset besar foto nyata. Algoritme menggunakan metadata foto EXIF yang direkam secara otomatis sebagai sinyal pengawasan untuk melatih model untuk menentukan apakah suatu gambar *self-consistent* - yaitu, apakah isinya dapat diproduksi oleh pipa pencitraan tunggal | Model *self-consistent* diterapkan untuk tugas mendeteksi dan melokalisasi splices gambar. Metode yang diusulkan memperoleh kinerja canggih pada beberapa tolok ukur forensik gambar, meskipun tidak pernah melihat gambar yang dimanipulasi di pembelajaran. |
| 2 | Fake Colorized Image Detection, 2018 [4] | Retouching | Histogram based Fake Colorized Image Detection (FCID-HIST) dan Feature Encoding based Fake Colorized Image Detection (FCID-FE) sebagai dua metode deteksi sederhana namun efektif untuk gambar berwarna palsu. | Hasil eksperimental menunjukkan bahwa kedua metode yang diusulkan menunjukkan kinerja yang layak terhadap beberapa pendekatan pewarnaan mutakhir. |
| 3 | BusterNet: Detecting Copy-Move Image Forgery with Source/Target Localization, 2018 [5] | Copy-Move | *Deep neural architecture* untuk *image copy-move forgery detection* (CMFD) yang diberi nama kode BusterNet yang dapat dilatih. Memiliki dua cabang arsitektur yang melokalkan daerah manipulasi potensial melalui artefak visual dan daerah *copy-move* melalui kesamaan visual. | BusterNet mengungguli algoritma pendeteksian *copy-move* canggih dengan margin besar pada dua dataset yang tersedia untuk umum, CASIA dan CoMoFoD, dan juga kuat terhadap berbagai serangan yang diketahui. |
| 4 | Learning Rich Features for Image Manipulation Detection, 2018 [6] | Multiple manipulation | Menggunakan dua aliran jaringan R-CNN yang lebih cepat (RGB stream dan noise stream) dan melatihnya ujung ke ujung untuk mendeteksi daerah yang dirusak | Eksperimen pada empat dataset manipulasi gambar standar menunjukkan bahwa dua aliran kerangka kerjanya mengungguli setiap aliran individu, dan juga |

| | | | | |
|---|---|---|---|---|
| | | | dengan gambar yang dimanipulasi | mencapai kinerja canggih dibandingkan dengan metode alternatif dengan kekuatan untuk mengubah ukuran dan kompresi. |
| 5 | Universal Image Manipulation Detection using Deep Siamese Convolutional Neural Network, 2018 [7] | Multiple manipulation | Metode yang diusulkan mengklasifikasikan tambalan gambar dalam mode pasangan-bijaksana secara sama atau berbeda menggunakan jaringan saraf siamese yang mendalam. Setelah jaringan mempelajari fitur yang dapat membedakan antara operasi pengeditan gambar yang berbeda, maka akan dapat membedakan antara operasi pengeditan gambar yang berbeda yang tidak ada dalam tahap pelatihan. | Hasil eksperimen menunjukkan kemanjuran metode yang diusulkan dalam mendeteksi / membedakan operasi penyuntingan gambar yang berbeda |
| 6 | Analysis of Copy Move Image Forgery Detection Using Histogram of Orientated Gradient, 2018 [8] | Copy-Move | Mendeteksi pemalsuan gambar menggunakan HOG (Histogram of Orientated Gradient). Pertama mentransfer gambar RGB ke gambar baca Grayscale, kemudian gambar Grayscale dibagi ke blok yang tumpang tindih. Terapkan HOG untuk mengekstraksi fitur, kemudian menyortir leksikografis dan melakukan proses pencocokan untuk mendeteksi wilayah pemalsuan, akhirnya menggambar wilayah duplikat. | Untuk evaluasi sistem dihitung Tingkat Positif, Tingkat Positif Palsu, dan Angka Identifikasi. |
| 7 | Pixel based Image Forensic Technique for copy-move forgery detection using Auto Color Correlogram, 2016 [9] | Copy-Move | Auto Color Correlogram (ACC), yang merupakan teknik ekstraksi fitur pengambilan gambar berbasis konten dengan kompleksitas rendah, digunakan untuk mendapatkan vektor fitur dari gambar yang dipalsukan. Dalam pemalsuan copy-move karena daerah yang dipalsukan memiliki gambar yang sama, maka | Skema ini berhasil mendeteksi daerah palsu yang diskalakan atau dirotasi saat menempel, juga secara efektif mendeteksi duplikasi beberapa wilayah dalam gambar. |

| | | | | |
|---|---|---|---|---|
| | | | akan membuat ketidakkonsistenan pada tingkat piksel di gambar yang diubah. | |
| 8 | Copy-Move Forgery Detection Using ORB and SIFT Detector, 2016 [10] | Copy-Move | Algoritma SVM (Support Vector Machine) dan EM (Expectation Maximization) digunakan untuk mengklasifikasikan data palsu dan non-palsu setelah ekstraksi fitur gambar menggunakan SIFT (Scale Invariant Feature Transform) dan ORB (Oriented FAST and rotated BRIEF). | Hasil percobaan menunjukkan kinerja yang lebih baik menggunakan metode ORB dengan SVM (Support Vector Machine) dan ORB dengan EM (Expectation Maximization) dalam hal Akurasi, Presisi, Recall dan F1 daripada SIFT dengan metode EM. |
| 9 | Segmentation Based On Image Copy Move Forgery Detection by Using Image Feature Matching, 2016 [11] | Copy-Move | Menemukan gambar duplikasi di dalam gambar asli dengan menggunakan penggalian metode titik kunci. Menggunakan dua tahap proses pencocokan, pertama adalah menemukan pasangan tambalan menggunakan matriks transformasi affine, kedua mencocokkan tambalan menggunakan teknik eksekusi iterasi loop. | Metode memiliki kinerja yang baik dengan mempercepat proses pencocokan dan mudah menemukan gambar palsu dibandingkan dengan metode pendeteksian pemalsuan lainnya. |
| 10 | Efficient Dense-Field Copy-Move Forgery Detection, 2015 [12] | Copy-Move | Algoritma baru untuk deteksi akurat dan lokalisasi pemalsuan copy-move, berdasarkan fitur invarian rotasi yang dikomputasi secara padat pada gambar PatchMatch, algoritme pencarian tetangga terdekat terdekat yang cepat sangat cocok untuk perhitungan bidang padat di atas gambar. | Analisis eksperimental, yang dilakukan pada database yang tersedia secara online, membuktikan teknik yang diusulkan setidaknya sama akurat, umumnya lebih kuat dan jauh lebih cepat daripada referensi canggih yang digunakan saat ini. |

Dari literature diatas paling banyak didapatkan paper deteksi manipulasi secara pasif dengan tipe copy-move, mungkin karena banyak ditemukan image manipulasi dengan metode ini. Dalam pemalsuan *copy-move*, satu wilayah disalin dan ditempelkan di atas wilayah lain dalam gambar yang sama untuk menyembunyikan beberapa informasi penting. Perbedaan *copy-move* dan *image splicing* adalah dalam media gambar yang digunakan untuk manipulasi, dalam *splicing* gambar, satu wilayah dipotong dan disisipkan di atas wilayah lain dalam gambar yang berbeda untuk membuat gambar baru.

Tabel 2. Ringkasan penjelasan deteksi manipulasi dan jumlah literatur

| Deteksi manipulasi | Penjelasan | Jumlah |
|---|---|---|
| Retouching | Dapat didefinisikan sebagai "pemolesan gambar", secara umum retouching mengacu pada peningkatan permukaan gambar | 1 |
| Image Splicing | Beberapa bagian gambar disalin dan ditempel pada gambar lainnya untuk mendapatkan gambar baru hasil manipulasinya | 1 |
| Copy-Move | Satu segmen gambar disalin dan ditempel di bagian lain dari gambar yang sama, tujuannya untuk menyembunyikan beberapa petunjuk visual atau mereplikasi hal-hal dalam gambar untuk menyesatkan orang | 6 |
| Multiple manipulation | Mengambil dua gambar termanipulasi sebagai input, dan memeriksa apakah tambalan itu berasal dari operasi manipulasi yang sama atau berbeda | 2 |

Dari berbagai metode yang di review, meskipun memberikan hasil deteksi yang baik tetapi tidak ada yang dapat memberikan hasil deteksi 100%, hasil deteksi bergantung dari spesifikasi citra yang akan diuji. Citra yang berbeda spesifikasinya akan memberikan hasil deteksi yang berbeda pula dari masing-masing metode yang digunakan. Oleh sebab itu dilihat dari penelitian ini masih membuka peluang metode lain untuk dapat ditemukan.

## 5. KESIMPULAN

Keaslian dan integritas citra digital menjadi sangat penting dalam berbagai bidang penerapan antara lain seperti forensik, pencitraan medis, e-commerce, industri fotografi, finance dan lain sebagainya. Pemeriksaan verifikasi keaslian dari citra sangat populer digunakan dimana citra dianggap sebagai bukti terkait hukum, catatan sejarah ataupun untuk tujuan klaim asuransi. Karena kemajuan teknologi dan ketersediaan perangkat lunak untuk manipulasi dan pemrosesan citra sudah demikian canggih, citra asli dapat dirusak tanpa meninggalkan jejak untuk mendeteksi pemalsuan. Studi ini menyimpulkan terdapat berbagai jenis pemalsuan citra dan pendekatan yang tersedia dan sudah diteliti khususnya dalam ilmu pengolahan citra digital atau *Digital Image Processing*. Untuk itu dalam meningkatkan keakuratan deteksi manipulasi citra artinya menyatakan apakah suatu citra asli atau tidak, maka perlu menggunakan lebih dari satu metode dan menggabungkannya untuk mendapatkan hasil deteksi yang lebih baik.

## REFERENSI

[1] K. B. Meena and V. Tyagi, *Image Forgery Detection: Survey and Future Directions*, no. September. 2019.

[2] B. Santhosh Kumar, S. Karthi, K. Karthika, and R. Cristin, "A systematic study of image forgery detection," *J. Comput. Theor. Nanosci.*, vol. 15, no. 8, pp. 2560–2564, 2018, doi: 10.1166/jctn.2018.7498.

[3] M. Huh, A. Liu, A. Owens, and A. A. Efros, "Fighting Fake News: Image Splice Detection via Learned Self-Consistency," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018, doi: 10.1007/978-3-030-01252-6_7.

[4] Y. Guo, X. Cao, W. Zhang, and R. Wang, "Fake Colorized Image Detection," *IEEE Trans. Inf. Forensics Secur.*, pp. 1–13, 2018, doi: 10.1109/TIFS.2018.2806926.

[5] Y. Wu, W. Abd-Almageed, and P. Natarajan, "BusterNet: Detecting copy-move image forgery with source/target localization," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018, doi: 10.1007/978-3-030-01231-1_11.

[6] P. Zhou, X. Han, V. I. Morariu, and L. S. Davis, "Learning Rich Features for Image Manipulation Detection," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2018, doi: 10.1109/CVPR.2018.00116.

[7] A. Mazumdar, J. Singh, Y. S. Tomar, and P. K. Bora, "Universal Image Manipulation Detection using Deep Siamese Convolutional Neural Network," *arXiv*, no. August 2018, pp. 1–6, 2018.

[8] A. T. Gaikwad, "Analysis of Copy

Move Image Forgery Detection Using Histogram of Orientated Gradient," *Int. J. Res. Eng. Appl. Manag.*, vol. 04, no. 06, pp. 33–36, 2018, doi: 10.18231/2454-9150.2018.0687.

[9] A. V. Malviya and S. A. Ladhake, "Pixel Based Image Forensic Technique for Copy-move Forgery Detection Using Auto Color Correlogram," *Procedia Comput. Sci.*, vol. 79, pp. 383–390, 2016, doi: 10.1016/j.procs.2016.03.050.

[10] R. Kaur and A. Kaur, "Copy-Move Forgery Detection Using ORB and SIFT Detector," *Int. J. Eng. Dev. Res.*, vol. 4, no. 4, pp. 804–813, 2016.

[11] B. R. M and R. Poovendran, "Segmentation Based On Image Copy Move Forgery Detection by Using Image Feature Matching," *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 5, no. 2, pp. 8–11, 2016.

[12] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient Dense-Field Copy-Move Forgery Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 11, pp. 2284–2297, 2015, doi: 10.1109/TIFS.2015.2455334.