TIN: Terapan Informatika Nusantara
Vol 1, No 12, Mei 2021, Hal 612-617
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

Analisa Deteksi Orisinalitas Citra Digital Menerapkan Metode Tiger

Puspa Sari

Program Studi Teknik Informatika Universitas Budi Darma, Medan, Indonesia
Email : puspasari0709@gmail.com

Abstrak−Perkembangan citra digital sekarang sangat pesat, hal tersebut membuat citra mudah untuk dibuat dan diedit. Dengan perkembangan tersebut banyak pihak yang menyalahgunakannya dengan memanipulasi citra. Pengolahan image pada citral digital dapat dibuat atau diedit dengan mudah, bahkan tanpa meninggalkan petunjuk visual oleh penggunaanya. Kemudahan dalam membuat dan merubah suatu citra dapat merusak kredibilitas keaslian image dalam berbagai aspek, sehingga membuat rawan digunakan untuk tindak kejahatan karena perubahan image pada citra digital dapat merubah informasi yang disampaikan menjadi berbeda. Hal ini menjadi dasar penelitian ini untuk mendeteksi keaslian suatu citra. Metode yang digunakan dalam melakukan pendeteksian orisinalitas citra adalah metode tiger, sesuai dengan fungsi utama dari fungsi hasing berfungsi untuk mengambil penanda dari sebuah citra yang nantinya akan dipakai sebagai acuan untuk memeriksa apakah suatu citra asli atau palsu. Perhitungan indeks akan dikonversikan ke dalam bentuk desimal agar diketahui jenis nilai indeks nya dan dilakukan perhitungan terhadap file yang akan dikoreksi dengan menggunakan matlab.

Kata Kunci: Orisinalitas; Citra; Tiger

Abstract−The development of digital images is now very fast, it makes images easy to create and edit. With this development, many people abuse it by manipulating images. Image processing in digital images can be created or edited easily, without even leaving visual clues to its use. The ease in creating and changing an image can damage the credibility of the authenticity of the image in various aspects, thus making it prone to be used for criminal acts because image changes in digital images can change the information conveyed to be different. This is the basis of this research to detect the authenticity of an image. The method used in detecting image originality is the tiger method, in accordance with the main function of the hashing function, which functions to retrieve a marker from an image which will later be used as a reference to check whether an image is real or fake. The index calculation will be converted into decimal form so that the type of index value is known and the calculation is carried out on the file which will be corrected using matlab.

Keywords: Originality; Image; Tiger

1. PENDAHULUAN

Perkembangan teknologi saat ini telah berkembang sangat cepat sehingga segala aktivitas dapat dilaksanakan oleh masyarakat umum dengan memanfaatkan media-media teknologi modern. Dampak negatif daripada perkembangan teknologi salah satunya adalah penyalahgunaan teknologi terhadap pemalsuan citra dan merubahnya sehingga citra menjadi tidak original atau palsu.Hal ini menyebabkan pengguna sebuah data sangat rumit untuk membedakan data yang asli dan data yang palsu, misalnya penggunaan citra digital. Keamanan dalam orisinalitascitraadalah hal yang harus diperhatikan dan tidak boleh diabaikan,karena orisinalitas citra digital atau dokumen dan bersifat penting dan tidak boleh dimanipulasi atau disalahgunakan oleh pihak lainnya[1]. Dengan cara inilah masyarakat luas mengembangkan bagaimana cara untuk mengamankan suatu citra digital untuk melihat orisinalitas data yang dimiliki dokumen tersebut. Salah satu upaya yang dapat dilakukan untuk menjaga orisinalitas file citra digital,maka diperlukan sebuah aplikasi yang memiliki kemampuan untuk melakukan deteksi terhadap keaslian sebuah citra digital dengan tujuan untuk membuktikan keasliannya. Mendeteksi orisinalitas citra digital merupakan salah satu proses untuk menemukan atau menentukan keberadaanatau kenyataan dari sebuah citra digital yang dilakukan secara komputerisasi.

Kriptografi adalah ilmu untuk menjaga suatu keamanan data. Kriptografi ini merupakan suatu metode pengamanan data yang dapat digunakan untuk menjaga orisinalitas data,serta kerahasiaan data tersebut.Teknik kriptografi terdiri dari simetris. Untuk mengetahui orisinalitas citra digital yang telah diubah kita dapat menggunakan metode Tiger.Menurut Ross Anderson dan Elli Biham pada tahun 1996. Fungsi ini dirancang sebagai fungsi hash MD dan SHA. Ketika ditemukannya collision pada algoritma MD dan SHA yang sangat terpercaya sudah bisa collisiondari sinilah mulai terbentuk suatu ide untuk membuat metode tiger.

Metode tiger diambil dari sifat metodenya yang sangat kuat dan cepat. Metode ini juga bisa dijalankan tidak hanya pada prosesor 32 bit,namun bisa juga bekerja pada prosesor 32 bit,namun bisa juga bekerja pada prosesor 16 dan 64 bit dengan sangat cepat. Prinsip kerja algoritma hash sebenarnya mirip dengan SHA. Pertama dilakukan padding message dimana pesan diubah menjadi kelipatan 512 bit. Untuk blok terakhir dilakukan padding dengan menambahkan bit 1 dan dilanjutkan dengan bit 0 hingga panjang message menjadi 448kemudian message tersebut ditambahkan dengan 64 bit yang mempresentasikan panjang pesan. Fungsi Tiger membutuhkan tiga buah penyangga yang terdiri dari 64 bit, total penyangga adalah 192 bit

2. METODOLOGI PENELITIAN

2.1 Pengolahan Citra

Pengolahan citra merupakan proses untuk menghasilkan citra sesuai dengan keinginan atau kualitasnya menjadi lebih baik. Inputannya adalah citra dan keluarannya juga citra tapi dengan kualitas lebih baik dari pada citra masukan. Misal

TIN: Terapan Informatika Nusantara
Vol 1, No 12, Mei 2021, Hal 612-617
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

citra warnanya kurang tajam, kabur *(blurring)* dan mengandung noise (misal bintik-bintik putih) sehingga perlu ada pemrosesan untuk memperbaiki citra karena citra tersebut menjadi sulit di interpretasikan karena informasi yang disampaikan menjadi berkurang[3-6].

2.2 Algoritma Tiger

Algoritma tiger adalah fungsi hash baru yang dirancang oleh Ross Anderson dan Elli Biham pada tahun 1996. Fungsi ini dirancang sebagai fungsi hash alternatif ketika ditemukannya collision pada fungsi hash MD dan SHA. Ketika ditemukannya collision pada algoritma MD dan SHA, banyak orang meragukan kekuatan fungsi hash lain mengingat MD dan SHA yang sangat terpercaya sudah bisa ditemukan collision. Dari sinilah mulai terbentuk suatu ide untuk membuat algoritma Tiger ini. Algoritma Tiger diambil dari sifat algoritmanya yang sangat kuat dan cepat. Algoritma ini juga bisa dijalankan tidak hanya pada prosesor 32 bit, namun bisa juga bekerja pada prosesor 16 dan 64 bit dengan sangat cepat. Prinsip kerja algortima hash ini sebenarnya mirip dengan SHA. Pertama dilakukan padding message dimana pesan diubah menjadi kelipatan 512 bit. Untuk blok terakhir dilakukan padding dengan menambahkan bit 1 dan dilanjutkan dengan bit 0 hingga panjang *message* menjadi 448, kemudian *message* tersebut ditambahkan dengan 64 bit yang merepresentasikan panjang pesan [2]. Ada beberapa faktor keamanan yang dipertimbangkan dalam penemuan algoritma Tiger ini, antara lain [1] :

1. Prinsip nonlinearity muncul kebanyakan dari S-box dengan jumlah 8 sampai 64 bit. Hal ini lebih baik dibandingkan jika kita hanya mengkombinasikan operasi penambahan dan operasi XOR (menggunakan carry bits), dan hal ini mengakibatkan efek pada semua bit keluaran bukan hanya bit tetangga saja.
2. Terdapat semacam longsoran yang kuat, dalam setiap bit pesan akan mengakibatkan efek semua tiga register setelah tiga putaran – lebih cepat daripada fungsi hash yang lain. Longsoran ini pada 64-bit words (dan 64-*bit S box)* berjalan dengan lebih cepat dibandingkan jika word yang lebih pendek digunakan.
3. Seperti yang telah dijelaskan di atas, semua serangan pada MD*/Snefru menargetkan pada salah satu blok intermediate, Dengan menaikkan nilai intermediate menjadi 192 bit membantu menghalangi terjadinya serangan ini.
4. *Key Schedule* memastikan bahwa perubahan pada sedikit jumlah bit pada pesan dapat mengakibatkan efek pada banyak bit yang muncul selama fase-fase selanjutnya. Bersama dengan point kedua di atas, hal ini membantu Tiger untuk melawan serangan yang sama dengan *Dobbertin's differential attack* pada MD4 (dimana merubah beberapa bit tertentu pada pesan dapat mengakibatkan efek pada paling banyak dua bit pada banyak putaran, dan perubahan kecil ini dapat dibuat untuk dibatalkan pada putaran terakhir).
5. Multiplikasi dari register b dalam setiap putaran juga berkontribusi untuk pertahanan terhadap serangan d atas, asalkan dipastikan bahwa bit yang dipakai sebagai masukan untuk S-box dalam putaran sebelumnya dicampurkan ke dalam S-box yang lain dengan baik, dan ke S-box yang sama dengan masukan yang berbeda. Multiplikasi ini juga mencegah *related-key attacks* pada fungsi *hash*, asalkan konstanta yang dipakai berbeda pada setiap putaran.
6. *Feedforward* yang digunakan dapat mencegah *meet-in-the-middle birthday attack* yang menemukan gambaran umum dari fungsi *hash* (meskipun kompleksitasnya akan menjadi sangat besar).

Kelebihan yang belum dimiliki oleh fungsi hash sebelumnya yaitu kecepatan. Jika dilihat dari strukturnya yang rumit, menjadikan algoritma tiger menjadi algoritma yang lambat, namun pada kenyataanya algoritma tiger masih bisa menyaingi kecepatan SHA dalam melakukan proses hash. Hal ini disebabkan penggunaan kotak S-Box yang mempersingkat pendefinisian register ketika ingin menambah kerumitan dalam putaran algoritma tiger.

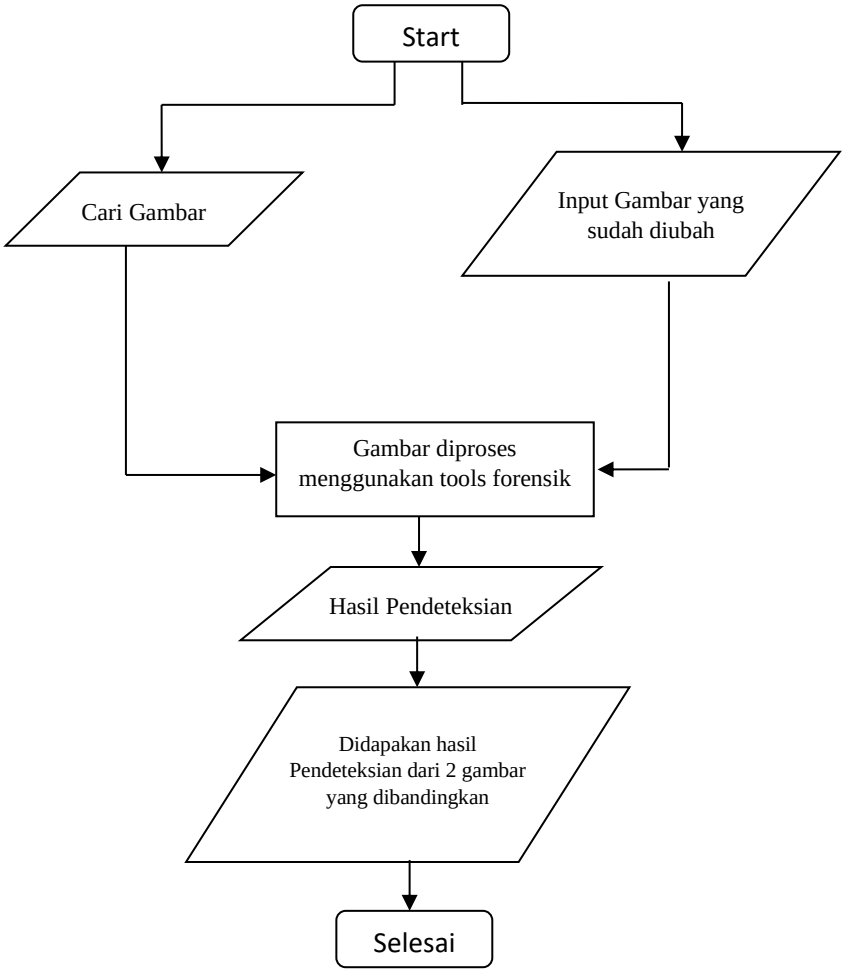
3. HASIL DAN PEMBAHASAN

Suatu gambar yang dilihat atau dijumpai terutama dalam dunia digital bisa saja adalah sebuah gambar yang telah dimanipulasi disebabkan oleh kecanggihan teknologinya dan perangkat lunak pengolah gambar dengan kelengkapan *tools* nya. Gambar palsu dapat dikategorikan sebagai penipuan walaupun tidak semua gambar palsu adalah hal yang buruk bisa saja sebagai hiburan. Motif yang paling berbahaya didalam menghasilkan gambar palsu adalah untuk mendapatkan keuntungan maupun mengubah persepsi masyarakat tentang sebuah kebenaran peristiwa. Untuk menghindari hal-hal tersebut diatas diperlukan suatu langkah yang dapat memberikan kepastian terhadap keaslian sebuah gambar. Salah satu solusi penyelesaian melakukan proses otentifikasi keaslian dari sebuah citra, sehingga dapat diketahui citra asli atau palsu.

3.1 Penerapan Metode Tiger

Pada penelitian ini menggunakan sebuah pembuatan rule sendiri untuk melakukan pendeteksian dalam mendapatkan suatu bukti digital yang digunakan untuk menganalisa crita digital tersebut. Skenario yang dibuat yaitu dengan menyiapkan dua *file image*, yang asli dan yang sudah dirubah. kemudian menginput *image* tersebut kedalam *tools forensik* dan dilakukan analisis pada dua image sehingga didapat hasil pendektisian dari dua *image* tersebut. Otentifikasi di dalam teknik pengamanan data dapat diterapkan dengan memanfaatkan fungsi hash dari sebuah citra. Konsep otentifikasi sebuah citra diawali dengan mencari sebuah citra.

TIN: Terapan Informatika Nusantara
Vol 1, No 12, Mei 2021, Hal 612-617
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin



Gambar 1. Alur Flowchart Proses Pendeteksian

Untuk melakukan pengujian maka dibutuhkan suatu sampel citra untuk mendeteksi keaslian citra tersebut. Adapun citra sampel dapat dilihat pada gambar dibawah ini.



(a) citra asli



(b) citra Splicing

Gambar 2. Citra Asli (a), Citra Splicing (b)

Citra yang dijadikan sampel pengujian adalah citra splicing (citra asli yang telah ditambahkan). Proses pendeteksian citra tersebut adalah dengan menggunakan metode tiger. Berdasarkan gambar diatas maka untuk nilai dari RGB dapat dilihat pada tabel 1 dibawah ini

Tabel 1. Nilai Sampel RGB

Piksel 1			Piksel 2			Piksel 3		
R	G	B	R	G	B	R	G	B
162	99	70	121	51	30	75	33	30

Citra berwarna (*RGB*) dikonversi ke dalam bentuk citra *grayscale.* Cara yang dapat digunakan untuk mengkonversi citra *RGB* ke citra *grayscale.* Nilai intensitas f_i^R, f_i^G dan f_i^B seperti berikut:

TIN: Terapan Informatika Nusantara
Vol 1, No 12, Mei 2021, Hal 612-617
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

$f_i^R = 1$
$f_i^G = 1$
$f_i^B = 1$
maka perhitungannya sebagai berikut :

$$f_o(y,x) = \frac{(1 \times 162) + (1 \times 121) + (1 \times 75)}{3}$$

= 162+121+75
= 357, karena jangkauan nilai intensitas warna 8 bit max 255 maka nilai intesitas 357 menjadi 255.
= 255/3
= 85

Untuk menghasilkan permutasi dari 256 kemungkinan *bytes* yang ada pada *array* S. Dimana S adalah permutasi 256-*byte* yang diinisialisasikan KSA, *variabel* i dan j merupakan *variabel integer* yang mempunyai nilai awal 0. Adapun *key* adalah kunci rahasia yang akan dimasukkan.

Tabel 2. S-Box

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	
239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

Untuk panjang kunci yang telah ditentukan sebelumnya akan dibuat dalam bentuk *array*. Untuk karakter dari kunci dapat dilihat pada tabel 3 dibawah ini.

Tabel 3. Jumlah Kunci

Indeks 0	Indeks 1	Indeks 2
N	I	A
78	73	65

Selanjutnya dilakukan pembentukkan array R sesuai dengan ketentuan yang telah ada.
Untuk i = 0
R[0] = Kunci [0 mod 3]
R[0] = Kunci [0] → N (dec 78)
Untuk i = 1
R[1] = Kunci [1 mod 3]
R[1] = Kunci [1] → I (dec 73)
Untuk i = 2
R[2] = Kunci [2 mod 3]
R[2]] Kunci [2] → A (dec 65)
Selanjutnya dilakukan proses nilai i = 255
R[255] = Kunci [255 mod 3]
R[255] = Kunci [0] → N (dec 78)
R[255] = Kunci [1] → I (dec 73)
R[255] = Kunci [2] → A (dec 65)
Sehingga menghasilkan nilan R keseluruhan dapat dilihat pada tabel 3.4 dibawah ini.

Tabel 4. Array R

78	73	65	78	73	65	78	73	65	78	73	65
78	73	65	78	73	65	78	73	65	78	73	65
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
78	73	65	78	73	65	78	73	65	78	73	65

Dengan menginisialisasikan nilai i, j, k, z dengan nilai 0 dan w merupakan nilai acak yang relatif prima dengan 256 dan setiap baris di modulo dengan 256. Hasil perhitungan pertama adalah:
Untuk i = 0, j = 0
j = (0 + S[0] + T[0]) mod 256
j = (0+0+78) mod 256
j = 78
Swap (S[0], S[78])

TIN: Terapan Informatika Nusantara
Vol 1, No 12, Mei 2021, Hal 612-617
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

j = 78

Tukarkan nilai tabel S-Box pada array 0 dengan nilai tabel S-Box pada array 78 dan begitu sebaliknya. Berdasarkan tabel 3.2, maka nilai S-Box[0] = 0 dan nilai S-Box[78] = 78. Jadi setelah ditukarkan, maka nilai S-Box[0] = 78 dan S-Box[78] = 0.

Untuk nilai i = 1 ; j = 78 (nilai akhir j pada iterasi i =0)
j = (78 + S[1]+T[1]) mod 256
j = (78 + 1 + 73) mod 256
j = 152 mod 256 = 152
Swap (S[1], S[152])
j = 78, nilai j selanjutnya adalah 78

Tukarkan nilai tabel S-Box pada array 1 (nilai i) dengan nilai tabel S-Box pada array 152 (nilai j) dan begitu sebaliknya. Pada proses permutasi ini, nilai tabel S-Box yang digunakan pada setiap proses swap (penukaran) adalah nilai S-Box setelah dipermutasikan. Proses permutasi ini dilakukan hingga nilai i = 255, sehingga proses ini dapat menyebabkan nilai array S-Box dapat di tukar secara berulang atau lebih dari satu kali.

1. Proses *Pseudo-Random Generation Algorithm (PRGA)*

Proses ini dilakukan untuk menghasilkan *key stream* yang akan digunakan pada proses tersebut. Proses iterasi pada PRGA dilakukan sebanyak jumlah nilai-nilai elemen warna citra. Bila citra sampel yang digunakan di atas memiliki 9 nilai, maka iterasi proses PRGA akan di lakukan sebanyak 9 kali. Pada Proses PRGA menyebabkan tabel permutasi S-Box akan dipermutasikan kembali sebanyak iterasi yang dilakukan pada proses ini.

Untuk iterasi 1, i = 0 ; j = 0
i = (0+1) mod 256 = 1
j = (0+S[1]) mod 256
j = (0+78) mod 256
j = 78
Swap (S[1], S[78])
Maka nilai S[1] = 152; S[78] = 86
t = (S[1]+S[78]) mod 256
t = (86 + 152) mod 256
t = 238 mod 256
t = 238
kunci [0] = S[238] → 162 (char ¶)
Untuk iterasi 2 → i=1; j=1
i = (1 + 1) mod 256 = 2
j = (1 + S-Box[2]) mod 256
j = (1 + 250) mod 256
j = 251
Swap (S-Box[2], S-Box[251])

Berdasarkan tabel S-Box (setelah permutasi iterasi 2 di atas), maka : nilai S-Box[2] = 250 dan S-Box[251] = 95 setelah ditukarkan menjadi : S-Box[2] = 95; S-Box[250] = 250. Iterasi selanjutnya dicari berdasarkan cara yang sama seperti di atas, sehingga di peroleh hasil dari *key stream*.

Untuk melakukan proses dari citra digital maka perlu dilakukan konversi nilai desimal dari piksel citra ke biner. Konversi nilai piksel dapat dilihat pada tabel 5 dibawah ini.

Tabel 5. Konversi Nilai Piksel Citra Ke Biner

Piksel	Warna	Desimal	Biner	P[i]
	R	162	10100010	P[1]
1	G	99	01100011	P[2]
	B	70	01000110	P[3]
	R	121	01111001	P[4]
2	G	51	00110011	P[5]
	B	30	00011110	P[6]
	R	75	01001011	P[7]
3	G	33	00100001	P[8]
	B	30	00011110	P[9]

Selanjutnya melakukan proses dengan nilai bit *Inisialization Vector* atau C0 : 01010010.

Blok P1 : i = 1
C1 = (P[1] ⊕ C[1-1)
= (P[1] ⊕ C[0])
= 10100010 ⊕ 01010010
= 11110000
Shift 2 bit dari kiri ke kanan (pemindahan 2 bit kiri ke kanan) C1 = 11000011 (dec 195)

TIN: Terapan Informatika Nusantara
Vol 1, No 12, Mei 2021, Hal 612-617
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

4. KESIMPULAN

Berdasarkan hasil penelitian dapat diberikan kesimpulan bahwa dalam mendeteksi orisinalitas citra digital yang menghasilkan citra *output* lebih baik adalah dengan menghitung rata-rata nilai dari citra yang rusak g(x,y) pada area yang didefinisikan oleh S_{xy}. Nilai dari citra $f(x,y)$ yang diperbaiki pada tiap titik (x,y) hanya dihitung dengan menggunakan *pixel* dalam daerah yang didefinisikan oleh $S_{xy.}$ Metode tiger dalam mendeteksi orisinalitas pada citra digital adalah menggunakan konvolusi di mana yang ditinjau hanyalah titik pusat S_{xy}saja, S_{xy} adalah *subimage* dari sebuah citra dan S_{xy} berukuran 5x5 yang mempunyai nilai berdasarkan hasil perhitungan $f\hat{}(x,y)$,

REFERENCES

[1] Respati, Dewangga, *"Studi Mengenai Algoritma Tiger Hash",* Makalah IF8029 Kriptografi, Program Studi Teknik Informatika, Institut Teknologi Bandung.
[2] Prama, I Nyoman, *"Pengembangan dan Implementasi Algoritma Tiger",* Makalah IF3058 Kriptografi, Semester II Tahun 2011/2012
[3] Komarudin, 2015, "Penerapan Algoritma", Penerbit Andi Offset, Yogyakarta.
[4] https://www.psychologymania.com/2013/04/pengertian-deteksi-dini.html, diakses tanggal 22 Juni 2019
[5] Amir Tjolleng, Pengantar Pemograman Matlab. Jakarta: PT Alex Media Kamputindo, 2017.
[6] T.Sutoyo, Edy Mulyanto, Vincent Suhartono, Oky Dwi Nurhayati, and Wijanarto, TEORI PENGOLAHAN CITRA DIGITAL. SEMARANG: ANDI, 2009