

Analisis Dan Implementasi Metode Patchwork Untuk Pengamanan Video

Yuliani Susiawati Hondro*, Sinar Sinurat

¹ Fakultas Ilmu Komputer dan Teknologi Informasi, Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: yulianisusiawatihondro@gmail.com

Abstrak—Dalam perkembangan informasi yang semakin pesat saat ini suatu informasi data yang dikirim atau diterima oleh seseorang sangatlah penting untuk dijaga kerahasiannya dan keberadaannya. Untuk itu sangatlah penting untuk meningkatkan keamanan data agar tidak dapat diketahui oleh orang lain yang tidak punya kepentingan supaya data kita tidak disalahgunakan untuk kepentingan diri sendiri. Salah satu penyebab penerapan watermarking adalah untuk memastikan sebuah objek yang di terima atau yang dimiliki adalah objek data asli, dan tidak dapat diketahui keberadaannya oleh orang lain. Manfaat dari pada watermarking untuk melindungi gambar, text, video, suara. Adapun tujuan lain dari watermarking yaitu untuk melindungi hak cipta kepemilikan dari suatu data atau informasi. Pada penelitian ini penulis akan melakukan analisis terhadap proses implementasi metode patchwork untuk pengamanan video. Metode Patchwork digunakan dalam watermarking dengan melakukan perhitungan statistik pada proses penyisipannya.

Kata Kunci: Analisis, Implementasi, Watermarking, Video, Patchwork.

Abstract—In the increasingly rapid development of information, data information sent or received by someone is very important to keep its confidentiality and existence. For this reason, it is very important to increase data security so that it is not known by other people who have no interest so that our data is not misused for their own interests. One of the reasons for applying watermarking is to ensure that an object that is received or owned is the original data object, and its existence cannot be known by others. Benefit from watermarking to protect pictures, text, video, sound. Another purpose of watermarking is to protect copyright ownership of data or information. In this study the authors will analyze the implementation process of the patchwork method for video security. The Patchwork method is used in watermarking by performing statistical calculations on the insertion process.

Keywords: Analysis, Implementasi, Watermarking, Video, Patchwork.

1. PENDAHULUAN

Analisis yang dilakukan dalam penelitian ini adalah berkaitan dengan pengimplementasian metode patchwork untuk pengamanan data jenis video. Kegiatan ini dilakukan karena begitu banyaknya data atau informasi yang dibagikan saat ini sudah menggunakan beberapa media digital informasi seperti aplikasi media sosial diantaranya facebook, twitter, whatsapp, instagram, messenger facebook dan lain-lain. Terkadang dengan pemanfaatan media ini sering menimbulkan beberapa kegiatan kejahatan yang dilakukan orang tidak bertanggung jawab terhadap informasi yang dibagikan. Bentuk kejahatan yang mungkin bisa terjadi seperti kegiatan penyadapan dan manipulasi terhadap data atau informasi. Maka dengan kondisi tersebut diperlukan sebuah teknik pengamanan yang mampu meminimalkan bahkan meniadakan terjadinya kejahatan.

Video merupakan salah satu jenis data pada umumnya sering digunakan untuk menyampaikan sebuah informasi kepada orang lain. Kandungan informasi yang ada dalam video terkadang mengandung informasi yang sifatnya rahasia, sehingga keamanannya perlu di jaga. Ketidakamanan pada video sering terjadi yaitu dapat di manipulasi dengan cara membuang beberapa bagian video sehingga informasi yang disampaikan melalui video tersebut tidak sesuai. Ini disebabkan karena adanya keberadaan video yang dapat diakses oleh semua orang. Maka untuk menghilangkan keberadaan video sebelum video tersebut didistribusikan atau dibagikan kepada orang yang berkepentingan, maka dibutuhkan sebuah teknik pengamanan yang disebut penerapan teknik watermarking.

Watermarking atau sering disebut dengan tanda air adalah teknik menyembunyikan data atau informasi yang sifatnya rahasia pada suatu media digital (gambar, suara, maupun video), tanpa disadari atau mampu tidak terlihat oleh mata biasa juga tahan terhadap proses – proses digitalisasi (editing media, baik noising, blurring, dan lain sebagainya) [1]. Salah satu metode watermarking yang dapat digunakan adalah Metode Patchwork.

Metode patchwork bekerja dalam watermarking dengan cara menggunakan perhitungan statistik didalam proses penyisipannya. Pada jurnal penelitian terdahulu yang dilakukan oleh P. Setiawan menuliskan bahwa pengujian terhadap metode patchwork dilakukan terhadap tingkat imperceptibility dan robustness dengan menggunakan acuan perhitungan PSNR, MOS, dan BER, yang meliputi kompresi image, zoom in, rotasi, brightness, dan color balance [2]. Maka melalui penulisan penelitian ini hasil yang diharapkan adalah sebuah hasil proses penerapan metode patchwork untuk pengamanan video dengan menggunakan watermarking image.

2. METODE PENELITIAN

2.1 Watermarking

Watermarking merupakan suatu bentuk dari steganography. Steganography adalah ilmu dan seni menyembunyikan pesan rahasia sedemikian sehingga keberadaan pesan tidak terdeteksi oleh indera manusia [9]. Watermarking (tanda air) ini sangat berbeda dengan tanda air yang ada dalam uang kertas. Tanda air yang ada dalam uang kertas masih bias dilihat oleh mata telanjang manusia, tetapi watermarking pada media digital dimaksudkan agar tidak dapat dirasakan kehadirannya oleh manusia tanpa alat bantu mesin pengolah digital seperti komputer dan sejenisnya. Watermarking ini memanfaatkan kekurangan-kekurangan sistem indera manusia seperti mata dan telinga.

Dengan adanya kekurangan inilah, metode watermarking ini dapat diterapkan pada berbagai media digital. Jadi watermarking merupakan suatu cara untuk menyembunyikan atau penanaman data/informasi tertentu (baik hanya berupa catatan umum maupun rahasia) ke dalam suatu citra digital lainnya, tetapi tidak diketahui kehadirannya oleh indera manusia (indera penglihatan dan pendengaran), dan mampu menghadapi proses-proses pengolahan sinyal digital sampai pada tahap tertentu [1]

2.2 Metode Patchwork

Teknik patchwork menggunakan metode redundant pattern encoding dan spread spectrum ke informasi tersembunyi yang tersebar dalam keseluruhan gambar cover ("patchwork" adalah metode yang menandai area gambar, atau patch). Dalam menggunakan redundant pattern encoding, harus menjual ukuran pesan melawan ketahanan. Untuk contoh, suatu pesan yang kecil dapat di gambarkan beberapa kali pada gambar sehingga jika stego-image di hasilkan, ada suatu kemungkinan yang tinggi bahwa watermark masih dapat terbaca. Suatu pesan yang besar dapat ditempelkan hanya sekali karena akan menduduki suatu porsi yang besar dari area gambar[12].

Metode patchwork ini akan menghasilkan citra rekonstruksi yang sangat mirip dengan aslinya, karena hanya mengubah bit tertentu dari citra. Misalkan suatu byte di dalam gambar mewakili warna tertentu, maka perubahan suatu bit tidak akan begitu mempengaruhi warna tersebut. Hal ini dikarenakan keterbatasan mata manusia dalam melihat perubahan warna tersebut. Sebagai contoh piksel 3x3 adalah[12]:

Tabel 1. Biner Citra

11110011,10110100,10011110	11001000,00110100,01111101	00111000,00101101,01010111
00011001,00101101,01111100	00001010,11001000,11111111	10011000,00010100,00100101
00111100,11100111,01001011	00111101,01010100,00010000	01011010,01110011,01011000

Sumber: Rudi Subrata, 2014 [12]

Penyisipan menggunakan patchwork dengan menandakan sebuah coverage area, kemudian penyisipan dilakukan dilakukan dengan mengganti 1 bit dari cover image. Teks yang disisipi berupa "DIA" di binerkan menjadi:

D = 01000100

I = 01001001

A = 01000001

Tabel 2. Biner Citra 3 x 3 disisipkan biner "DIA"

11110010,10110101,10011110	11001000,00110100,01111101	00111000,00101100,01010110
00011001,00101100,01111100	00001011,11001000,11111110	10011001,00010100,00100101
00111100,11100110,01001010	00111100,01010100,00010001	01011010,01110011,01011000

Sumber: Rudi Subrata, 2014 [12]

Untuk rumus penyisipan patchwork dapat dilakukan dengan cara di bawah ini:

$$X_{n+1} = (aX_0 + c) \bmod p \dots\dots\dots (1)$$

dimana X_{n+1} , adalah bilangan acak yang dihasilkan. p adalah jumlah pixel dikali 3 (tiga), dimana tiap piksel citra 24 bit memiliki tiga komponen warna yaitu red, green dan blue masing-masing 1 byte (8 bit). a adalah nilai karakter kata kunci kedua sebagai pengali (multiplier) c adalah nilai karakter kata kunci ketiga penambah (increment) X_0 adalah nilai karakter kata kunci pertama nilai awal (seed or start value).

3. HASIL DAN PEMBAHASAN

3.1 Analisa Masalah

Analisis adalah langkah dalam menyelesaikan pemecahan suatu masalah dari awal sampai akhir agar lebih mudah dimengerti. Analisis yang dilakukan dalam penelitian ini pertama dilakukan pemaparan yang berkaitan dengan bagaimana teknik pengamanan video yang dilakukan. Adapun jenis ekstensi file video yang akan dijadikan sebagai objek untuk menerapkan teknik pengamanan watermarking adalah mp4. Sementara untuk objek citra watermarknya menggunakan citra ekstensi JPEG.

Metode Patchwork adalah metode watermarking yang dapat digunakan untuk memberikan pengamanan terhadap video. Adapun langkah-langkah proses penerapan metode patchwork dapat diuraikan menjadi beberapa poin sebagai berikut:

1. Menentukan video dengan ekstensi mp4 yang akan diamankan
2. Menentukan citra watermark dalam hal ini menggunakan gambar dengan ekstensi JPEG
3. Melakukan ekstrasi nilai biner pada video, dan terhadap citra watermark
4. Melakukan proses encoding metode patchwork.

3.1.1 Penerapan Metode Patchwork

Nama Video : Sandi ATM
Durasi : 5 Detik
Ekstensi : MP4
Resolusi : 720 * 1280



Gambar 1. Tampilan Video

Nama Gambar : IMG_20200409_19328
Ekstensi : JPG
Ukuran : 3840 * 5120

Gambar 2. Tampilan Citra Watermak

Setelah watermark image JPEG dan video Mp4 ditentukan, langkah selanjutnya melakukan proses ekstraksi nilai hexadecimal pada masing-masing objek dengan menggunakan aplikasi “PX Binary Viewer”.

Data View		
Done, Identifier: DATA		
Address (Dec)	Hexadecimal (1 Byte)	Text (ASCII)
000876400	99 51 43 55 48 57 FD 32 F0 37 52 71 A4 ED D1 70 W	Q C U k w * 3 + ?
000876414	DE 66 8A 5B 17 2B 28 29 31 11 83 48 18 3D A8	* * * * * + * (9)
000876432	A3 86 79 4E 45 C3 54 05 45 BE 2B AC 08 DE 16 59	* * * y H * * * *
000876448	BD 15 DA A7 7B 0C 7B 97 CF 42 39 11 C8 8E FC DC	* * * * * (*) * * *
000876464	C1 07 40 6D 8A 87 17 CB CA 41 0F 65 37 45 E2 0D	* * * * * 8 * * * *
000876480	73 66 FC 64 31 5D 01 C3 38 41 87 3F 33 1F FC 0C	* * * * * f * d * * *
000876496	77 0C 1F 2D 58 41 88 C3 E2 84 3C 24 58 54 5B 10	* * * * * / - * A * * *
000876512	3C 38 94 EC 15 81 48 A3 82 50 27 76 26 A4 8B 1D	* * * * * * * * * *
000876528	0A 04 06 47 73 E2 6F 1B 5D 0C 8B 18 0A 0D C7	* * * * * G * * * * *
000876544	48 3E A6 C7 08 28 19 4E 4C D6 8E 4A 12 37 FC F2	* * * * * * * * * *
000876560	7D 0E 52 D2 D8 4E 83 83 03 06 D6 84 8E F9 23	* * * \ * * * H * * *
000876576	3D BE 91 A5 5D 3F 1A 45 4A ED 32 1F 59 6C FF 33	* * * * * * * * * *
000876592	BA A6 D6 A3 53 28 74 C5 46 7B 0C 8E A1 DF 24 CE	* * * * * * * * * *
000876608	70 A5 28 18 7B 8E 4A 45 DF A3 87 64 A2 3F 62 21	* * * * * * * * * *
000876624	97 C1 C6 35 87 1A 64 3D 9C 1A 4E 0D 10 05 84 51	* * * * * S * * * * *
000876640	DF CE 41 5E 24 FF 14 E7 0C 8B A5 16 34 E6 20	* * * * * A * * * * *
000876656	AD 10 55 71 87 27 27 33 05 38 4F A3 A6 1B 2A 34	* * * * * U q w * * *
000876672	CE F7 1C 0C 8E 8A 51 5E 78 C4 4F AF 86 A4 D0 12	* * * * * * * * * *
000876688	DB BE DB 5B FC A1 23 84 6C 7C BE 38 4E 64 58 67	* * * * * * * * * *
000876704	38 3E 94 47 67 A4 46 0A 03 09 82 D3 K7 F7 68	* * * * * g * F * *
000876720	FE 6E 30 53 8F 93 89 04 33 3D 41 DC 05 AB E7	* * * * * 0 * * * *
000876736	1D 5A 15 7B 1E F2 FC 8B 3A F0 5B 7B E5 70 10	* * * * * 2 * * * *
000876752	28 91 56 D3 4E A6 45 39 40 93 5C 76 FC 8B 15	* * * * * V * * * *
000876768	B1 9D 1D 89 74 A8 30 2D 5F 14 FB 35 06 D0 75 3F	Q * * * * *

Gambar 3. Nilai hexadecimal gambar sample

Dari gambar di atas sample data yang digunakan di ambil dari Address gambar 000876400 dengan banyak item nilai hexa yang diambil sebanyak 3, yaitu 77 51 43.

Address (Dec)	Hexadecimal (1 Byte)	Text (ASCII)
000000192	31 38 30 37 00 6D 73 6D 38 39 33 37 5F 36 34 2D	1 8 0 7 * m s m 8
000000208	75 73 65 72 20 38 2E 31 2E 30 20 4F 50 4D 31 2E	u s e r 8 . 1 .
000000224	31 37 31 30 31 39 2E 30 32 36 20 65 6E 67 2E 63	1 7 1 0 1 9 . 0 2
000000240	6F 6D 70 69 6C 2E 32 30 32 30 30 33 30 36 2E 31	o m p i l . 2 0 2
000000256	30 34 31 32 33 20 72 65 6C 65 61 73 65 2D 6B 65	0 4 1 2 3 . r e l
000000272	79 73 00 32 30 32 30 3A 30 34 3A 30 39 20 31 39	y s * 2 0 2 0 : 0
000000288	3A 33 32 3A 32 38 00 00 00 00 48 00 00 00 01 00	: 3 2 : 2 8 * * *
000000304	00 00 48 00 00 00 01 00 1F 92 7C 00 02 00 00 00	* H * * * * *
000000320	02 31 00 00 00 88 27 00 03 00 00 00 01 02 79 00	* 1 * * * * *
000000336	00 88 22 00 03 00 00 00 01 00 00 00 00 82 9D 00	* * " * * * * *
000000352	05 00 00 00 01 00 00 02 A5 82 9A 00 05 00 00 00	* * * * * * *
000000368	01 00 00 02 AD A2 17 00 03 00 00 00 01 00 02 00	* * * * * * *
000000384	00 92 92 00 02 00 00 00 07 00 00 02 B5 92 91 00	* * * * * * *
000000400	02 00 00 00 07 00 00 02 BC 92 90 00 02 00 00 00	* * * * * * *
000000416	07 00 00 02 C3 92 0A 00 05 00 00 00 01 00 00 02	* * * * * * *
000000432	CA 92 09 00 03 00 00 00 01 00 00 00 00 92 08 00	* * * * * * *
000000448	04 00 00 00 01 00 00 00 00 92 07 00 03 00 00 00	* * * * * * *
000000464	01 00 02 00 00 92 86 00 02 00 00 00 02 31 00 00	* * * * * * *
000000480	00 A4 06 00 03 00 00 00 01 00 00 00 00 A0 05 00	* * * * * * *
000000496	04 00 00 00 01 00 00 03 12 A4 05 00 03 00 00 00	* * * * * * *
000000512	01 00 1C 00 00 90 04 00 02 00 00 00 14 00 00 02	* * * * * * *
000000528	D2 A0 03 00 04 00 00 00 01 00 00 14 00 A4 03 00	* * * * * * *
000000544	03 00 00 00 01 00 00 00 00 92 03 00 0A 00 00 00	* * * * * * *
000000560	01 00 00 02 E6 90 03 00 02 00 00 00 14 00 00 02	* * * * * * *

Gambar 4. Nilai hexadecimal video

Gambar di atas adalah nilai hexadecimal frame video yang akan digunakan sebagai sampel data. Adapun address hexa video yang digunakan mulai dari alamat decimal 000 000 192 dengan banyak item hexa yang diambil sebanyak 27 item, yaitu

Nilai 1: 31, 38, 30

Nilai 2: 37, 00, 6D

Nilai 3: 73, 6D, 38

Nilai 4: 39, 33, 37

Nilai 5: 5F, 36, 34

Nilai 6: 2D, 75, 73

Nilai 7: 65, 72, 20

Nilai 8: 38, 2E, 31

Nilai 9: 2E, 30, 20

Langkah selanjutnya melakukan proses penerapan metode patchwork untuk mengamankan video. Berikut data biner citra watermark yang digunakan.

Tabel 3. Nilai biner hexadecimal citra watermark

Hexadecimal	Binner
77	01110111
51	01010001
43	01000011

Tabel 4. Nilai biner hexadecimal video

Nilai	Hexadecimal	Binner
1	31	00110001
	38	00111000
	30	00110000
2	37	00110111
	00	00000000
	6D	01101101
3	73	01110011
	6D	01101101
	38	00111000
4	39	00111001
	33	00110011
	37	00110111
5	5F	01011111
	36	00110110
	34	00110100
6	2D	00101101
	75	01110101
	73	01110011
7	65	01100101
	72	01110010

Nilai	Hexadecimal	Binner
8	20	00100000
	38	00111000
	2E	00101110
9	31	00110001
	2E	00101110
	30	00110000
	20	00100000

Setiap nilai pada tabel diatas telah direpresentasikan dengan nilai sebanyak 24 bit, untuk menampung nilai biner citra watermark yang di masukan ke dalam biner video. Untuk teknik penyisipan pengamanan metode patchwork dilakukan dengan cara mengganti 1 bit dari biner video dengan biner citra watermark. Nilai biner hexadecimal citra dari sample data Address 000876400 yang akan disisipkan adalah “ 77 51 43” yang telah dibinnerkan pada tabel sebelumnya.

77 = 01110111

51 = 01010001

43 = 01000011

Berikut hasil penyisipan biner gambar seperti pada tabel dibawah ini.

Tabel 5. Nilai biner hasil dari proses penyisipan

Piksel	Hexadecimal	Binner
1	31	00110000
	38	00111001
	30	00110001
2	37	00110111
	00	00000000
	6D	01101101
3	73	01110011
	6D	01101101
	38	00111000
4	39	00111001
	33	00110010
	37	00110111
5	5F	01011110
	36	00110110
	34	00110100
6	2D	00101101
	75	01110100
	73	01110011
7	65	01100100
	72	01110010
	20	00100000
8	38	00111000
	2E	00101111
	31	00110001
9	2E	00101110
	30	00110000
	20	00100000

Setelah proses penyisipan biner dilakukan, selanjutnya melakukan proses pengacakan terhadap biner. Proses pengacakan tersebut bergantung pada kata kunci (password) yang menjadi random seed atau titik awal dilakukannya pengacakan. Kata kunci yang dimasukkan merupakan nilai biner hexadecimal citra watermark yaitu “77, 51, 43” dengan asumsi biner video 9 X 24 dengan total byte yang dimiliki adalah 216 byte. Berikut merupakan nilai desimal dari kata kunci yang digunakan:

Tabel 6. Nilai Desimal Kunci

Hexadecimal	Decimal	Binner
77	119	01110111
51	81	01010001
43	67	01000011

Berikut rumus menentukan tata letak posisi penyimpanan biner dengan menggunakan rumus dibawah ini :

$$X_{n+1} = (aX_0 + c) \bmod p$$

dimana X_{n+1} , adalah bilangan acak yang dihasilkan. p adalah jumlah pixel dikali 3 (tiga), dimana tiap pixel citra 24 bit memiliki tiga komponen warna yaitu red, green dan blue masing-masing 1 byte (8 bit). a adalah nilai karakter kata kunci kedua sebagai pengali (multiplier) c adalah nilai karakter kata kunci ketiga penambah (increment).

X_0 adalah nilai karakter kata kunci pertama nilai awal (seed or start value), berdasarkan hasil penyisipan Nilai biner hexadecimal gambar ke nilai biner hexadecimal video $3 * 3$, maka:

$$X_1 = (77 \times 51 + 43) \bmod 216$$

$$X_1 = 82$$

$$X_2 = (82 \times 51 + 43) \bmod 216$$

$$X_2 = 121$$

$$X_3 = (121 \times 51 + 43) \bmod 216$$

$$X_3 = 166$$

$$X_4 = (166 \times 51 + 43) \bmod 216$$

$$X_4 = 85$$

$$X_5 = (85 \times 51 + 43) \bmod 216$$

$$X_5 = 58$$

$$X_6 = (58 \times 51 + 43) \bmod 216$$

$$X_6 = 193$$

$$X_7 = (193 \times 51 + 43) \bmod 216$$

$$X_7 = 166$$

$$X_8 = (166 \times 51 + 43) \bmod 216$$

$$X_8 = 85$$

Setelah penghitungan selesai dilakukan, langkah berikutnya adalah memasukkan nilai tersebut sebagai alamat posisi biner kunci, berikut adalah posisinya bit dari kunci nilai biner hexadecimal citra watermark yaitu "77 51 43" di bawah ini: 01110111 01010001 01000011

Tabel 7. Hasil lokasi byte penyisipan kunci

Bit "77 51 43"	Lokasi Byte Penyisipan
0	82
1	121
1	166
1	85
0	58
1	193
1	166
1	85
0	82
1	121
0	166
1	85
0	58
0	193
0	166
1	85
0	82
1	121
0	166
0	85
0	58
0	193
1	166
1	85

Maka setelah posisi penempatan kunci telah ditentukan maka proses pengamanan metode patchwork telah selesai. Dari hasil proses penyisipan juga memberikan perubahan nilai kapasitas terhadap video sebagai objek yang di amankan dengan teknik watermarking menjadi bertambah.

4. KESIMPULAN

Adapun beberapa poin kesimpulan yang diperoleh dari pembahasan Bab sebelumnya Metode patchwork dapat digunakan untuk proses pengamanan video. Dari hasil implementasi yang dilakukan terhadap metode patchwork untuk pengamanan video tidak merusak bentuk video awal maupun tidak terlalu mempengaruhi ukuran awal data. Metode Patchwork dapat diterapkan untuk mengamankan video dengan kapasitas yang berbeda-beda

REFERENCES

- [1] I. Aulia, "IMPLEMENTASI TEKNIK WATERMARKING PADA CITRA DIGITAL DENGAN MENGGUNAKAN METODE FRACTAL DAN DISCRETE COSINE TRANSFORM (DCT)," Jur. Teknik Inform. STMIK Budidarma Medan, vol. 6, 2019.
- [2] P. N. D. Setiawan, "Analisis dan Implementasi Steganography dengan Metode Patchwork pada Citra Digital," Telekomunikasi, 2009.
- [3] M. A. Hapsari, "Studi Steganografi pada Image File," Jur. Tek. Inform. ITB, 2010.
- [4] Makinuddin and T. H. Sasongko, Analisis Sosial Bersaksi Dalam Advokasi Irigasi, i. Bandung: Yayasan AKATIGA, 2006.
- [5] H. Al Fatta, Analisis dan Perancangan Sistem Informasi. Yogyakarta: Andi Publisher, 2007.
- [6] A. Firdianti, Implementasi Manajemen Berbasis Sekolah, 1st ed. Yogyakarta: CV. Gre Publishing, 2018.
- [7] D. U. B. Sore and Sobirin, Kebijakan Publik, 1st ed. Maksiar: Cv. Sah Media, 2017.
- [8] E. Setiawan, Kamus Buku Besar Indonesia. Badan Pengembangan dan Pembinaan Bahasa, 2012.
- [9] I. P. H. Wiguna, "IMPLEMENTASI BLIND WATERMARKING PADA CITRA DIGITAL DENGAN TRANSFORMASI WAVELET HAAR," Jur. Mat. Fak. MIPA, Univ. Udayana, Denpasar - Bali, vol. 1, 2015.
- [10] Fahmi, "STUDI DAN IMPLEMENTASI WATERMARKING CITRA DIGITAL DENGAN MENGGUNAKAN FUNGSI HASH," Tek. Inform. ITB, 2007.
- [11] W. T. Handoko and D. A. Diartono, "PERLINDUNGAN KEASLIAN CITRA DENGAN TEKNIK WATERMARKING," vol. VII, 2002.
- [12] R. Subrata, "PERANCANGAN APLIKASI WATERMAKING MENERAPKAN METODE PATCWORK," Pelita Inform. Budi Darma, vol. 7, no. 1, 2014.
- [13] I. 2005, "MPEG-4 File Formats white paper," in Archive, I., archive.org, 2008.
- [14] A. Nugroho, Rekayasa Perangkat Lunak Menggunakan UML & Java, I. Yogyakarta: Andi Offset, 2010.
- [15] Sahyar, Algoritma dan Pemrograman Menggunakan MATLAB (Matrix Laboratory). 2016.