BAB V . IMPLEMENTASI DAN PENGUJIAN

5.1 Implementasi Perhitungan Patchwork

Dalam implementasi proses patchwork ini dimana pesan akan disisipkan dalam bit-bit gambar (dengan asumsi bahwa pixel pada gambar yaitu 24 bit) dengan contoh gambar implementasi yaitu :

Gambar 5. 1 Gambar yang Akan disisipi pesan

Dicontohkan dengan pesan yang akan di kirim yaitu "POLINEMA" degan deret biner sebagai berikut dan table binary gambar yang akan disisipi pesan :

Tabel 5. 1 Tabel Binary Pesan

Text	ASCII	Biner
P	80	01010000
O	79	01001111
L	76	01001100
I	73	01001001
N	78	01001110

E	69	01000101
M	77	01001101
A	65	01000001

Pesan yang telah dirubah binary nantinya akan disisipkan pada gambar yang juga akan dirubah menjadi binary. Pesan yang akan disisipkan nantinya akan menggantikan bit terakhir dari kode biner suatu citra. Pada prosesnya,penggantian dilakukan dengan memilih byte tertentu secara acak tergantung pada kata kunci (password) yang menjadi titik awal pengacakan dengan citra ukuran X, Y (360, 640) dengan total byte yang dimiliki 691200. Berikut contoh kata kunci yang dimasukkan :

Tabel 5. 2 Tabel Binary Password

	A	**B**	**C**
ASCII	65	66	67
Biner	01000001	01000010	01000011

Dengan pesan dan password di atas, maka akan digunakan rumus penyisipan patchwork sebagai berikut [2]:

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

Dengan keterangan :

X_{n+1} : Bilangan acak yang dihasilkan

P : jumlah pixel dikali 3 (RGB)

a : nilai karakter kata kunci kedua (*multiplier*)

c : nilai karakter kata kunci penambah (*increment*)

X_0 : nilai karakter kata kunci pertama (*seed or start value*)

Sehingga dengan menggunakan rumus tersebut akan didapat :

X1 = (65 x 66 + 67) mod 691200

X1 = 4357

Perhitungan dilakukan secara berulang hingga bilangan password terakhir dan menempatkan bit dari pesan yang dikirim ke dalam bit citra :

Tabel 5. 3 Perhitungan Penyisipan Patchwork

X_{n+1}	$aX_0 + c$	Mod p (Lokasi Byte Penyim-panan)	Bit "POLI NEMA"	X_{n+1}	$aX_0 + c$	Mod p (Lokasi Byte Penyim-panan)	Bit "POLI NEMA"
1	4357	4357	0	33	21026941	290941	0
2	287629	287629	1	34	19202173	539773	1
3	18983581	321181	0	35	35625085	373885	0
4	21198013	462013	1	36	24676477	484477	0
5	30492925	80125	0	37	31975549	180349	1
6	5288317	449917	0	38	11903101	152701	1
7	29694589	664189	0	39	10078333	401533	1
8	43836541	290941	0	40	26501245	235645	0
9	19202173	539773	0	41	15552637	346237	0
10	35625085	373885	1	42	22851709	42109	1
11	24676477	484477	0	43	2779261	14461	0
12	31975549	180349	0	44	954493	263293	0
13	11903101	152701	1	45	17377405	97405	0
14	10078333	401533	1	46	6428797	207997	1
15	26501245	235645	1	47	13727869	595069	0
16	15552637	346237	1	48	39274621	567421	1
17	22851709	42109	0	49	37449853	125053	0
18	2779261	14461	1	50	8253565	650365	1
19	954493	263293	0	51	42924157	69757	0
20	17377405	97405	0	52	4604029	456829	0
21	6428797	207997	1	53	30150781	429181	1
22	13727869	595069	1	54	28326013	678013	1
23	39274621	567421	0	55	44748925	512125	0

X_{n+1}	$aX_0 + c$	Mod p (Lokasi Byte Penyim - panan)	Bit "POLI NEMA"
24	37449853	125053	0
25	8253565	650365	0
26	42924157	69757	1
27	4604029	456829	0
28	30150781	429181	0
29	28326013	678013	1
30	44748925	512125	0
31	33800317	622717	0
32	41099389	318589	1

X_{n+1}	$aX_0 + c$	Mod p (Lokasi Byte Penyim - panan)	Bit "POLI NEMA"
56	33800317	622717	1
57	41099389	318589	0
58	21026941	290941	1
59	19202173	539773	0
60	35625085	373885	0
61	24676477	484477	0
62	31975549	180349	0
63	11903101	152701	0
64	10078333	401533	1

Perhitungan yang telah diselesaikan (menentukan bit ke lokasi byte penyimpanan) kemudian memasukkan nilai tersebut ke dalam bit citra. Dalam bagian ini, ditentukan lokasi byte penyimpanan untuk dimasukkan ke dalam bit citra yang akan digantikan. Citra yang sebelumnya diubah dalam bentuk biner untuk diproses akan dikembalikan dalam bentuk citra lagi.

Untuk membaca pesan, maka proses dilakukan dengan cara terbalik dari proses penyisipan pesan pada citra. Proses dimuali dengan memasukkan password dan menghitung lokasi pesan dari password yang dimasukkan dengan contoh password "ABC" seperti berikut :

Tabel 5. 4 Tabel Password Ektraksi

	A	B	C
ASCII	65	66	67
Biner	01000001	01000010	01000011

Dari password tersebut akan dihitung dengan rumus patchwork yang sama untuk menemukan lokasi pesan yang disimpa. Dengan rumus patchwork berikut [2]:

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

Dengan keterangan :

X_{n+1} : Bilangan acak yang dihasilkan

P : jumlah pixel dikali 3 (RGB)

a : nilai karakter kata kunci kedua (*multiplier*)

c : nilai karakter kata kunci penambah (*increment*)

X_0 : nilai karakter kata kunci pertama (*seed or start value*)

Sehingga dengan menggunakan rumus tersebut akan didapat :

X1 = (65 x 66 + 67) mod 691200

X1 = 4357

X2 = (4357 x 66 + 67) mod 691200

X2 = 287629

Perhitungan dilakukan secara berulang hingga bilangan password terakhir dan menempatkan bit dari pesan yang dikirim kemudian akan terlihat nilai pixel tempat penyisipan pesan untuk melihat pesan yang telah disisipkan.

Tabel 5. 5 Tabel Ektraksi

X_{n+1}	**$aX_0 + c$**	**Mod p (Lokasi Byte Penyim - panan)**	**Biner Pixel**	**Bit Terakhir Pixel**	**Pesan**
1	4357	4357	11001000	0	**P**
2	287629	287629	10101101	1	
3	18983581	321181	01100100	0	
4	21198013	462013	11001001	1	
5	30492925	80125	10111100	0	
6	5288317	449917	10011000	0	
7	29694589	664189	00001000	0	
8	43836541	290941	10000000	0	
9	19202173	539773	01001100	0	**O**

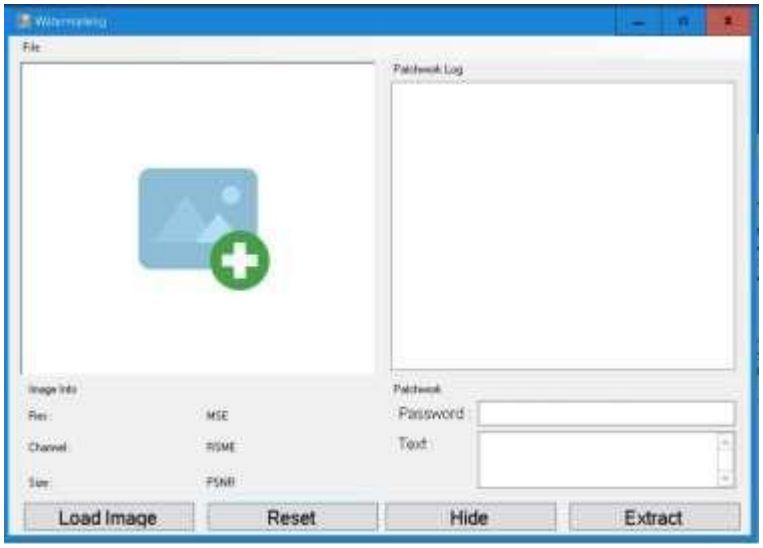
X_{n+1}	$aX_0 + c$	Mod p (Lokasi Byte Penyim - panan)	Biner Pixel	Bit Terakhir Pixel	Pesan
10	35625085	373885	01100101	1	
11	24676477	484477	01010110	0	
12	31975549	180349	11010110	0	
13	11903101	152701	11000001	1	
14	10078333	401533	01000101	1	
15	26501245	235645	11011001	1	
16	15552637	346237	10011001	1	
17	22851709	42109	10101110	0	
18	2779261	14461	10100101	1	
19	954493	263293	11101000	0	
20	17377405	97405	00100100	0	**L**
21	6428797	207997	11011011	1	
22	13727869	595069	10001111	1	
23	39274621	567421	00000010	0	
24	37449853	125053	01101100	0	
25	8253565	650365	01001000	0	
26	42924157	69757	11110101	1	
27	4604029	456829	11101110	0	
28	30150781	429181	11001000	0	**I**
29	28326013	678013	10101101	1	
30	44748925	512125	01100100	0	
31	33800317	622717	11001000	0	
32	41099389	318589	10111101	1	
33	21026941	290941	10011000	0	
34	19202173	539773	00001001	1	
35	35625085	373885	10000000	0	
36	24676477	484477	01001100	0	**N**
37	31975549	180349	01100101	1	
38	11903101	152701	01010111	1	
39	10078333	401533	11010111	1	
40	26501245	235645	11000000	0	
41	15552637	346237	01000100	0	
42	22851709	42109	11011001	1	
43	2779261	14461	10011000	0	**E**
44	954493	263293	10101110	0	
45	17377405	97405	10100100	0	

X_{n+1}	$aX_0 + c$	Mod p (Lokasi Byte Penyim - panan)	Biner Pixel	Bit Terakhir Pixel	Pesan
46	6428797	207997	11101001	1	
47	13727869	595069	00100100	0	
48	39274621	567421	11011011	1	
49	37449853	125053	10001110	0	
50	8253565	650365	00000011	1	
51	42924157	69757	01101100	0	
52	4604029	456829	01001000	0	**M**
53	30150781	429181	11110101	1	
54	28326013	678013	11101111	1	
55	44748925	512125	11001000	0	
56	33800317	622717	10101101	1	
57	41099389	318589	01100100	0	
58	21026941	290941	11001001	1	
59	19202173	539773	10111100	0	
60	35625085	373885	10011000	0	
61	24676477	484477	00001000	0	**A**
62	31975549	180349	10000000	0	
63	11903101	152701	01001100	0	
64	10078333	401533	01100101	1	

Dari perhitungan patchwork maka ditemukan lokasi pixel tempat penyisipan pesan sehingga akan terlihat pesan dari bit terakhir nilai biner pixel yang akan ditemukan pesan awal yang disisipkan seperti contoh yaitu pesan “POLINEMA”.

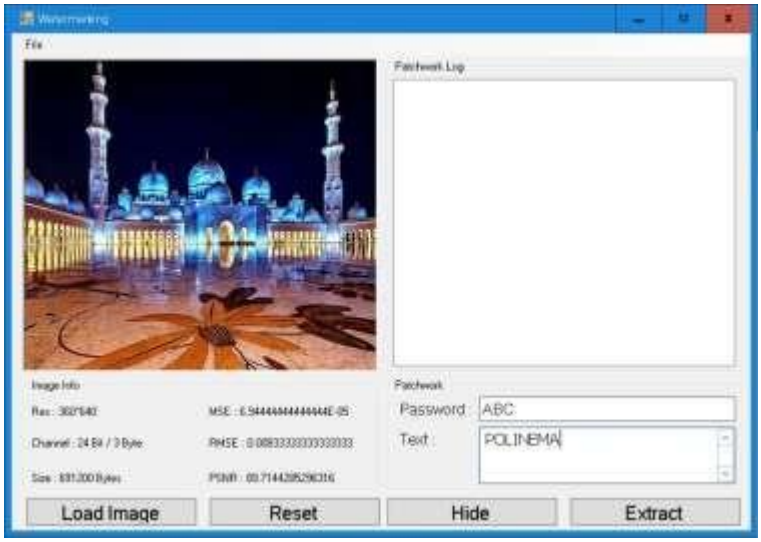
5.2 Implementasi Antarmuka

Dalam implementasi ini, menunjukkan antaramuka sistem yang dibangun. Dalam antarmuka terdapat fitur unggah gambar yang bisa muncul ketika di klik pada box gambar.

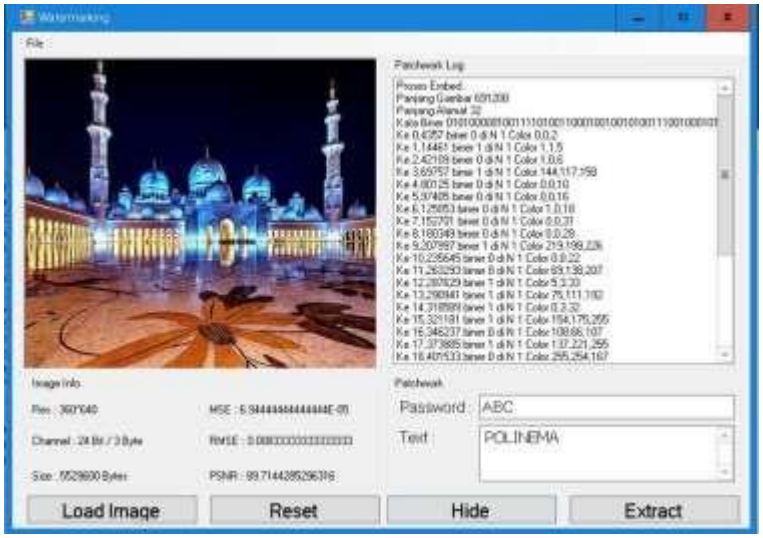


Gambar 5. 2 Upload Gambar

Gambar yang telah diunggah akan dimunculkan pada sistem dan user bisa menginputkan password serta pesan yang akan disisipkan melalui bit-bit pada gambar yang kemudian bisa memilih button hide sehingga sistem bisa memproses penyisipan pesan pada gambar.



Gambar 5. 3 Input Password dan Pesan



Gambar 5. 4 Tampilan Extract

5.3 Pengujian Sistem

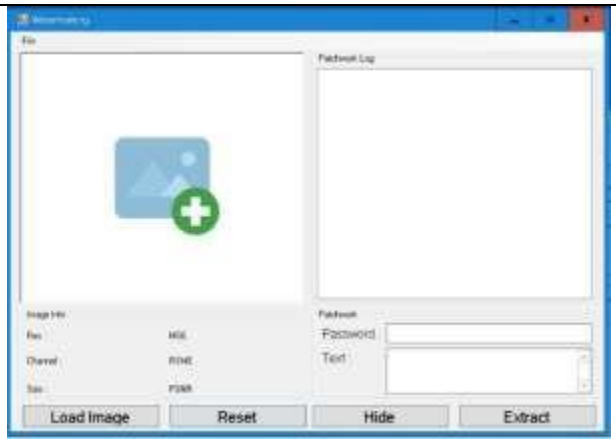
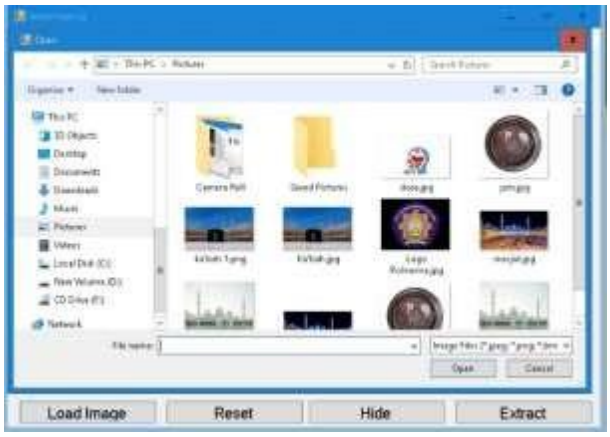
Pengujian sistem dilakukan dengan menggunakan metode *blackbox* dan pengecekan PSNR gambar setelah gambar disisipn pesan seperti berikut :

5.3.1 Blackbox

1. Upload Gambar

Tabel 5. 6 Upload Gambar

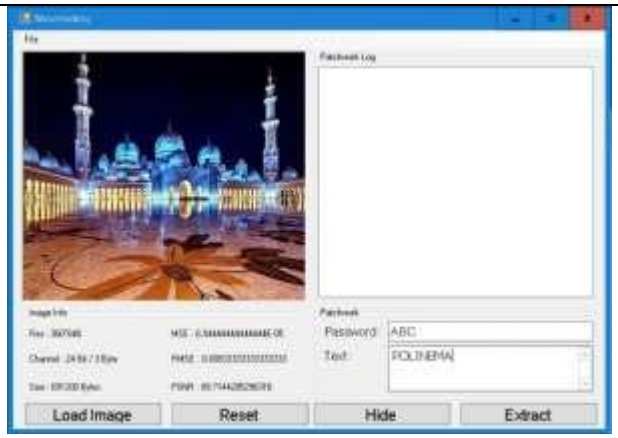
Hasil Pengujian	
Nama Fungsi	*Upload* Gambar
Data Masukan	Gambar yang akan disisipi pesan
Hasil yang Diharapkan	Gambar muncul pada sistem
Hasil Pengujian	Gambar muncul pada sistem

Screenshoot	 
Kesimpulan	Berhasil

2. Input Password dan Pesan

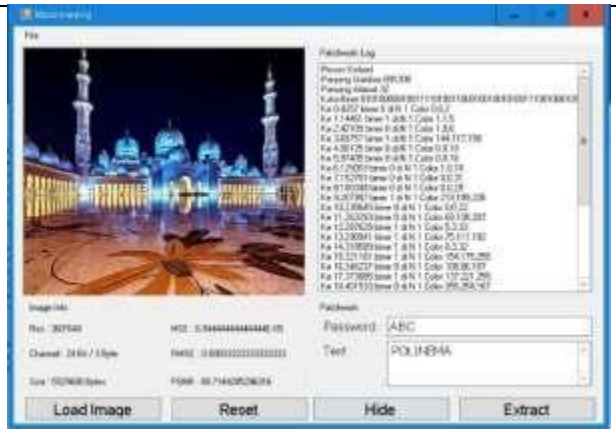
Tabel 5. 7 Input Password dan Pesan

Hasil Pengujian	
Nama Fungsi	Input Password dan Pesan
Data Masukan	Password dan pesan
Hasil yang Diharapkan	User bisa menginputkan password dan pesan
Hasil Pengujian	Password dan pesan bisa diinputkan pada sistem

Screenshoot	
Kesimpulan	Berhasil

3. Hide (Proses Waterwarking dan Patchwork)

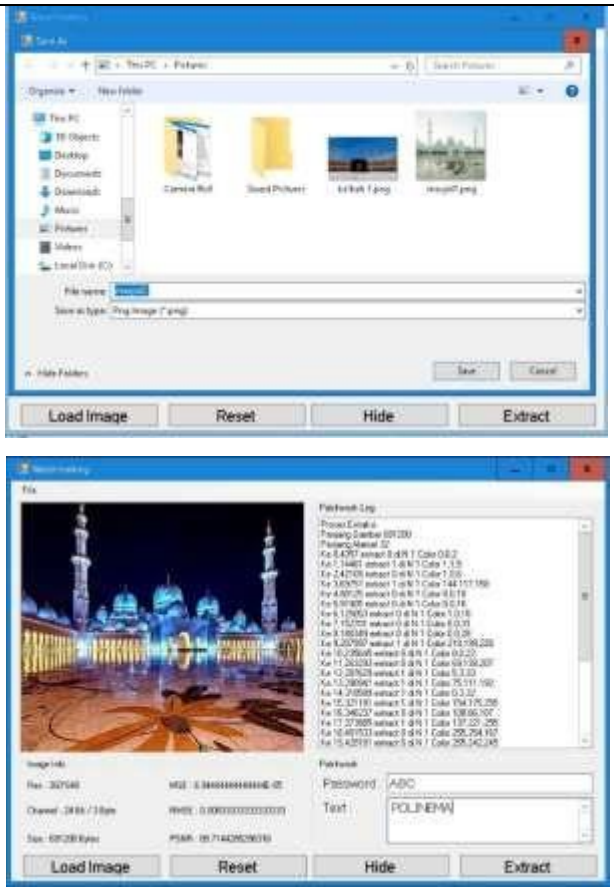
Tabel 5. 8 Hide (Proses Watermarking dan Patchwork)

Hasil Pengujian	
Nama Fungsi	Hide (Proses Waterwarking dan Patchwork)
Data Masukan	Gambar yang akan disisipi pesan
Hasil yang Diharapkan	Gambar bisa disisipi pesan
Hasil Pengujian	Indikator berhasil menyisipkan pesan
Screenshoot	
Kesimpulan	Berhasil

4. Extract

Tabel 5. 9 Extract

Hasil Pengujian	
Nama Fungsi	*Extract*

Data Masukan	Gambar yang telah melalui proses watermarking dan patchwork
Hasil yang Diharapkan	Pesan muncul setelah proses input gambar dan password
Hasil Pengujian	Pesan berhasil muncul
Screenshoot	
Kesimpulan	Berhasil

5.3.2 Pengecekan PSNR

Peak signal to noise ratio (PSNR) merupakan sebuah parameter yang biasa digunakan dalam proses kompresi image untuk menentukan kualitas hasil rekonstruksi image akhir. Selain PSNR dijadikan sebagai parameter pengukuran kualitas hasil rekonstruksi image, perbandingan nilai rasio kompresi warna dan mean square error (MSE) dijadikan pembanding untuk melihat korelasi yang terjadi antara ketiga parameter ini terhadap kualitas image hasil rekonstruksi[11].

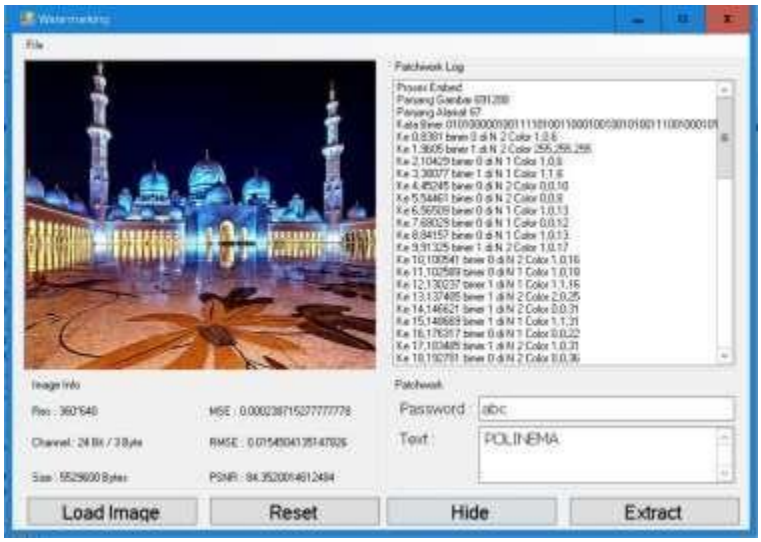
Pada penelitian ini, penulis melakukan uji coba dengan memasukkan citra dan password yang sama tetapi dengan pesan yang berbeda. Dari uji coba tersebut dihasilkan data sebagai berikut :

Pada proses penyisipan pesan “POLINEMA” dengan password “ABC” dihasilkan :

MSE : 0.000238715277777778 dB

RMSE : 0.0154504135147826 dB

PSNR : 84.3520014612484 dB



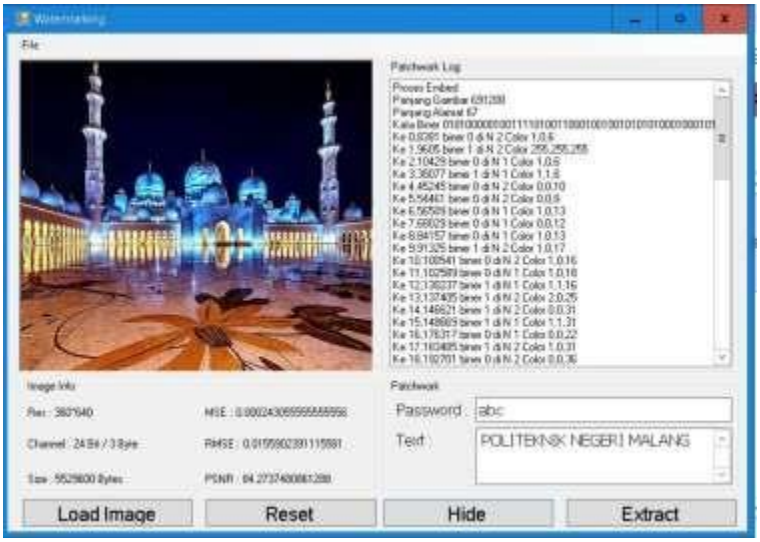
Gambar 5. 5 Penyisipan Pesan "POLINEMA"

Pada proses penyisipan pesan “POLITEKNIK NEGERI MALANG” dengan password “ABC” dihasilkan :

MSE : 0.000243055555555556 dB

RMSE : 0.0155902391115581 dB

PSNR : 84.2737480861288 dB



Gambar 5. 6 Penyisipan Pesan "POLITEKNIK NEGERI MALANG"