BAB 6

KESIMPULAN DAN SARAN

Pada bab ini, akan dijelaskan kesimpulan dari awal hingga akhir penelitian beserta saran untuk penelitian selanjutnya.

6.1 Kesimpulan

Skema (n, n)-NVSS merupakan pengembangan dari skema konvensional VSS yang bertujuan untuk mengurangi *transmission risk* yang muncul saat proses transmisi *share* dilakukan. *Share* yang digunakan dalam skema ini adalah $n - 1$ *natural share* dan satu *share* tidak bermakna, di mana proses transmisi *share* tidak bermakna tersebut membutuhkan media yang aman. Media yang digunakan dalam penelitian ini adalah *QR Code*.

Kesimpulan dari penelitian ini didapat setelah melakukan beberapa langkah. Berikut adalah langkah-langkah yang dilakukan:

1. Telah dipelajari cara kerja skema (n, n)-NVSS.
2. Telah dipelajari cara untuk menyembunyikan *share* tidak bermakna ke dalam *QR Code*.
3. Telah diimplementasikan skema (n, n)-NVSS dan cara penyembunyian *Share* tidak bermakna ke dalam *QR Code*.

Berdasarkan pengujian fungsional yang telah dilakukan pada Subbab 5.2, dapat disimpulkan bahwa perangkat lunak yang dibangun dapat mengimplementasikan skema (n, n)-NVSS dengan menggunakan *QR Code* sebagai media transmisi. Perangkat lunak juga dapat merekonstruksi gambar rahasia dengan hasil yang mirip dengan gambar rahasia yang digunakan.

Berdasarkan pengujian eksperimental yang telah dilakukan pada Subbab 5.3, dapat disimpulkan bahwa *parameter* yang mempengaruhi kualitas *share* tidak bermakna secara signifikan adalah penggunaan *natural share* yang memiliki warna dominan yang sama atau mirip, di mana kualitas terbaik dihasilkan oleh *natural share* dengan warna dominan gelap. Nilai probabilitas kemunculan *noise* juga mempengaruhi kualitas *share* yang dihasilkan, di mana kualitas terbaik dihasilkan dengan menggunakan nilai tertinggi dalam percobaan, yaitu 0.9. Pengaruh nilai blok piksel dalam kualitas *share* yang dihasilkan lebih rendah jika dibandingkan dengan pengaruh nilai probabilitas kemunculan *noise* dan penggunaan jenis *natural share* yang berbeda.

Pengujian dengan menggunakan ukuran *natural share* yang berbeda juga menunjukkan pengaruh terhadap *QR Code* yang dihasilkan. Semakin besar ukuran *natural share* maka *QR Code* yang dihasilkan juga menjadi semakin besar dan kompleks di mana ukuran maksimal gambar yang dapat digunakan adalah 30×30 piksel. Hal ini disebabkan oleh batas *QR Code* dan metode kompresi yang digunakan. Metode kompresi yang digunakan hanya dapat melakukan kompresi pada gambar dengan ukuran maksimal 30×30 piksel yang hasil kompresinya masih dapat dimasukkan ke dalam *QR Code*. Hasil kompresi untuk gambar yang ukurannya lebih besar dari 30×30 piksel tidak dapat dimasukkan ke dalam *QR Code*.

6.2 Saran

Berikut adalah saran untuk penelitian selanjutnya:

- Pada penelitian ini, perangkat lunak yang dibangun hanya mampu untuk memasukkan data ke dalam *QR Code* dengan ukuran maksimal 30×30 piksel. Untuk penelitian selanjutnya, penulis berharap perangkat lunak dikembangkan untuk dapat memasukkan gambar ke dalam *QR Code* dengan ukuran yang lebih besar atau menggunakan media lain sebagai media transmisinya.
- Pada penelitian ini, gambar yang digunakan sebagai *natural share* hanya bertipe gambar *soft-copy*. Untuk penelitian selanjutnya, penulis berharap perangkat lunak dikembangkan untuk dapat memproses gambar *hard-copy* juga.
- Pada penelitian ini, kasus-kasus yang diuji masih kurang beragam. Untuk penelitian selanjutnya, penulis berharap lebih banyak kasus dapat diuji.

DAFTAR REFERENSI

[1] Wang, M.-S. dan Chen, W.-C. (2008) Robust copyright protection scheme based on discrete cosine transform and secret sharing techniques. *Journal of Electronic Imaging*, **17(2)**.

[2] Lee, K.-H. dan Chiu, P.-L. (2014) Digital image sharing by diverse image media. *ieee transactions on information forensics and security*, **9**, 88–98.

[3] Naor, M. dan Shamir, A. (1995) Visual cryptography. *Advances in Cryptology EUROCRYPT'94*, pp. 1–12. Springer.

[4] Ateniese, G., Blundo, C., De Santis, A., dan Stinson, D. R. (2001) Extended capabilities for visual cryptography. *Theoretical Computer Science*, **250**, 143–161.

[5] Wu, X., Ou, D., Liang, Q., dan Sun, W. (2012) A user-friendly secret image sharing scheme with reversible steganography based on cellular automata. *Journal of Systems and Software*, **85**, 1852–1863.

[6] Nissar, A. dan Mir, A. (2010) Classification of steganalysis techniques: A study. *Digital Signal Processing*, **20**, 1758–1770.

[7] Munir, R. (2006) *Kriptografi*. Informatika, Bandung.

[8] Provos, N. dan Honeyman, P. (2003) Hide and seek: An introduction to steganography. *IEEE security & privacy*, **99**, 32–44.

[9] Al-Najjar, Y. A. dan Soong, D. C. (2012) Comparison of image quality assessment: Psnr, hvs, ssim, uiqi. *International Journal of Scientific & Engineering Research*, **3**, 1.