

BAB 6

KESIMPULAN DAN SARAN

Pada bab ini akan dibahas kesimpulan dari awal hingga akhir penelitian dan saran untuk penelitian selanjutnya.

6.1 Kesimpulan

Bagian ini akan membahas kesimpulan dari seluruh penelitian yang dilakukan pada skripsi ini. Kesimpulan diperoleh setelah melakukan beberapa langkah pengerjaan. Berikut merupakan langkah-langkah pengerjaan yang sudah dilakukan untuk memperoleh kesimpulan.

1. Mempelajari *secret sharing*, skema VSS, *random grids*, VSS Naor Shamir, RIVSS dengan teknik *random grids*, dan metode pemisahan *background* dan *foreground*.
2. Mengimplementasikan skema RIVSS dengan teknik *random grids* secara manual.
3. Mengimplementasikan skema $(2, n)$ -VSS Naor Shamir, $(3, n)$ -VSS Naor Shamir, Tradisional VSS dengan teknik *random grids*, dan RIVSS dengan teknik *random grids* pada perangkat lunak.

Berdasarkan langkah-langkah pengerjaan yang telah dilakukan dan berdasarkan pengujian pada Subbab 5.2, didapatkan kesimpulan bahwa perangkat lunak yang dibangun oleh penulis sudah dapat mengimplementasikan proses memasukan gambar rahasia lalu membuat *shadow* sesuai dengan jenis VSS dan proses menampilkan *shadow* serta melakukan penumpukan shadow.

Berdasarkan pengujian pada Subbab 5.3, diperoleh kesimpulan bahwa metode VSS dengan Teknik *Random Grids* dibanding VSS Naor Shamir lebih baik karena nilai euclidean distance lebih kecil pada kasus pengujian eksperimental dengan gambar solid dengan batas gambar tegas (jumlah segmen = 1), pengujian eksperimental dengan gambar solid dengan batas gambar tegas berpola abjad.

Sedangkan untuk kasus pengujian eksperimental dengan gambar solid dengan batas gambar tegas (jumlah segmen = 2), pengujian eksperimental dengan gambar solid dengan batas gambar tegas (jumlah segmen = 3), dan pengujian eksperimental dengan gambar solid dengan batas gambar tidak tegas, VSS Naor Shamir lebih baik dibandingkan VSS dengan Teknik *Random Grids* karena nilai *euclidean distance* lebih kecil

Sehingga tidak dapat didefinisikan skema mana yang lebih baik karena kedua skema ini dapat sama-sama lebih baik tergantung dari contoh kasus berdasarkan input gambar, nilai k dan n serta besarnya ukuran gambar.

VSS dengan Teknik *Random Grids* memiliki kelebihan yaitu skema ini tidak memiliki ekspansi piksel sehingga besar ukuran gambar rahasia dengan *shadow* tidak berbeda dibandingkan dengan skema VSS Naor Shamir yang besar ekspansi piksel nya berbanding lurus dengan besar nilai n . Selain itu, teknik VSS dengan Teknik *Random Grids* ini dapat digunakan ketika suatu gambar rahasia akan dibagi ke dalam beberapa *region* yang memang tidak ingin mampu direkonstruksi semuanya sebelum nilai n tercapai walau nilai k sudah tercapai.

6.2 Saran

Pada bagian ini akan dibahas saran dari penulis untuk pengembangan penelitian ini lebih lanjut. Berikut merupakan saran-saran tersebut.

- Pada penelitian ini, VSS dengan Teknik *Random Grids* hanya menangani input gambar rahasia berupa gambar biner. Untuk penelitian lebih lanjut, penulis berharap perangkat lunak dapat dikembangkan sehingga bisa menangani input gambar rahasia yang lain yaitu gambar *grayscale* dan gambar berwarna.
- Pada penelitian ini, batasan segmen untuk batas gambar yang tidak tegas hanya menangani 1 segmen saja (misal : foto wajah satu orang saja). Untuk penelitian lebih lanjut, penulis berharap perangkat lunak dapat dikembangkan sehingga bisa menangani input gambar rahasia yang lebih dari 1 segmen untuk batas gambar yang tidak tegas.

DAFTAR REFERENSI

- [1] Shamir, A. (1979) How to share a secret. *Communications of the ACM*, **22**, 612–613.
- [2] Naor, M. dan Shamir, A. (1995) *Visual cryptography*. In *Proceedings of Advances in Cryptology (EUROCRYPT 94)* volume 950. Springer-Verlag, Berlin.
- [3] Kafri, O. dan Keren, E. (1987) Encryption of pictures and shapes by random grids. *Optics Letters*, **12**, 377–379.
- [4] Wang, R.-Z. (2009) Region incrementing visual cryptography. *IEEE Signal Processing Letters*, **16**, 659–662.
- [5] Kumar, S. dan Sharma, R. K. (2015) Random-grid based region incrementing visual secret sharing. *Fundamenta Informaticae*, **137**, 369–386.
- [6] Burger, W. dan Burge, M. J. (2009) Regions in binary images. Bagian dari Mackie, I. dan Polytechnique, E. (ed.), *Principles of Digital Image Processing - Core Algorithm*. Springer, United Kingdom.
- [7] Open cv library. <https://opencv.org/about.html>. November 2018.