

ABSTRAK

Kerahasiaan data merupakan hal yang penting dalam bidang teknologi informasi seperti saat ini. Dalam kasus tertentu, terdapat keadaan dimana sebuah instansi mempunyai data rahasia yang harus dibagi kepada beberapa orang, dan untuk mengaksesnya dibutuhkan pecahan sebanyak jumlah tertentu, sehingga data rahasia dapat direkonstruksi kembali menjadi data awal. Permasalahan ini dapat diselesaikan dengan menggunakan skema *k-n Visual Cryptography*. Pada penelitian ini, *file* rahasia dienkripsi dengan metode *Tiny Encryption Algorithm (TEA)* dan *file* terenkripsi dipecah menjadi *n* pecahan dengan membagikan bit 1 secara acak ke beberapa pecahan *file*. Untuk merekonstruksi *file* atau mengembalikan *file* awal, maka dibutuhkan minimal *k* pecahan. Proses penggabungan menggunakan fungsi OR, kemudian hasil penggabungan didekripsi dengan metode TEA. Aplikasi dapat digunakan untuk mengamankan data atau *file* rahasia dengan cara mengenkripsinya menggunakan metode TEA dan memecahnya dengan menggunakan skema *k-n Visual Cryptography*. Sesuai pengujian, proses penggabungan berjalan lebih cepat dibandingkan proses pemecahan, dan keberhasilan proses penggabungan mencapai 100% bila kunci dekripsi sama dengan kunci enkripsi dan jumlah pecahan yang digabung lebih besar atau sama dengan nilai *k*.

Kata Kunci: Pengamanan, *File*, TEA, *Visual Cryptography*, Enkripsi, Dekripsi, *Secret Sharing*

ABSTRACT

Data confidentiality is important in information technology as it is today. In certain cases, there are circumstances which an agency has confidential data that must be shared among several people, and to access the data, it requires a certain amount of fraction or share, so that the data can be reconstructed back to the original data. This problem can be solved by using Visual Cryptography k-n scheme. In this study, secret file is encrypted by Tiny Encryption Algorithm (TEA) method and the encrypted file is broken into n fractions by sharing bit 1 randomly into several file fractions. To reconstruct the file or to restore the original file, it takes at least k fraction. The merge process uses the OR function, and the result is decrypted by TEA method. Application can be used to secure confidential data or files by encrypting them using TEA method and breaking them using the Visual Cryptography k-n scheme. According to testing made, the reconstruction process runs faster than the splitting process, and the success of the reconstruction process reaches 100% if the decryption key is same as the encryption key and the number of fractions merged is greater than or equal to the value of k.

Keywords: Security, File, TEA, Visual Cryptography, Encryption, Decryption, Secret Sharing