Jurnal Riset Komputer (JURIKOM), Vol. 5 No. 4, Agustus 2018
ISSN 2407-389X (Media Cetak)
Hal: 357-361

# Algoritma *Blowfish* Pada Watermarking Video Digital

**Mufida Khairani, Nurwulan**

Universitas Harapan Medan, Medan, Indonesia
email: mufida.khairani@gmail.com

**Abstrak**

Penggunaan format digital terutama pada data video, suara atau musik masih menimbulkan kontroversi seputar perlindungan hak ciptanya. Permasalahan tersebut menyebabkan pentingnya suatu pembuktian kepemilikan atas hak cipta dari suatu media digital. Untuk dapat membuktikan kepemilikan atas hak cipta, dapat digunakan teknik watermarking. Pada penelitian ini digunakan metode algoritma blowfish untuk watermarking video digital menggunakan aplikasi VB.Net. Penelitian ini bertujuan untuk melindungi hak cipta pemilik video digital dengan menerapkan algoritma blowfish sehingga meningkatkan robustness watermarking yang ada pada video digital tersebut. Hasil dari penelitian ini berupa aplikasi program yang dapat digunakan oleh semua pihak. Karena aplikasi ini sangat user friendly.

**Kata Kunci**: Kriptografi, Watermarking, Blowfish, Video Digital

**Abstract**

The use of digital formats, especially in video, voice or music data, is still causing controversy surrounding the protection of copyright. These problems cause the importance of proof of ownership of the copyright of a digital media. To be able to prove ownership of copyright, watermarking techniques can be used. In this study, the blowfish algorithm method is used for digital video watermarking using the VB.Net application. This study aims to protect the copyright of digital video owners by applying the blowfish algorithm so as to increase the watermarking robustness that exists in the digital video. The results of this study are application programs that can be used by all parties. Because this application is very user-friendly.

**Keywords**: Cryptography, Watermarking, Blowfish, Digital Video

## 1. PENDAHULUAN

Penggunaan format digital terutama pada data video, suara atau musik masih menimbulkan kontroversi seputar perlindungan hak ciptanya. Kemudahan pengolahan data digital menyebabkan sering terjadi pelanggaran hak cipta data tersebut. Sering terjadi penduplikasian, pengambilan sebagian atau seluruh isi data, maupun pendistribusian secara ilegal terhadap data digital tanpa melalui izin dari pemiliknya, sehingga secara otomatis pemilik hak cipta telah dirugikan atas perbuatan tersebut.

Permasalahan tersebut menyebabkan pentingnya suatu pembuktian kepemilikan atas hak cipta dari suatu media digital. Untuk dapat membuktikan kepemilikan atas hak cipta, dapat digunakan teknik *watermarking*. *Watermarking* merupakan teknik yang digunakan untuk menyembunyikan tanda atau informasi hak cipta seperti waktu atau tanggal, dan pemilik hak cipta ke dalam suatu media digital[6]. Penyisipan informasi ke dalam video digital dilakukan sedemikian rupa sehingga tidak merusak kualitas video yang disisipi informasi hak cipta. Informasi hak cipta ini harus dapat diekstrak untuk membuktikan kepemilikan atas produk video digital tersebut. Hasil dari proses ekstraksi kemudian dibandingkan dengan informasi asli dari pemegang hak cipta. Jika informasi hasil ekstraksi sama dengan informasi asli maka dialah pemegang hak cipta atas produk video digital tersebut.

Untuk membuat watermarking tersebut digunakanlah algoritma blowfish. Algoritma blowfish adalah cipher blok yang berarti selama proses enkripsi dan dekripsi, blowfish bekerja dengan membagi pesan menjadi blok-blok bit dengan ukuran sama panjang, yaitu 64-bit dengan panjang kunci bervariasi yang mengenkripsi data dalam 8 byte blok [1].

Pada penelitian (Utami, et.al, 2010) implementasi algoritma *Blowfish* yang optimal dapat dilakukan dengan aplikasi yang tidak sering berubah-ubah kunci serta tidak menggunakan *weak-key*. Dalam fungsi F terdapat total 521 iterasi untuk menghasilkan semua subkunci yang dibutuhkan. Aplikasi kemudian dapat menyimpan subkunci ini dan tidak membutuhkan langkah-langkah proses penurunan berulang kali, kecuali kunci yang digunakan berubah. [1]

Berdasarkan penelitian yang sudah pernah dilakukan oleh peneliti lain dan dari uraian di atas penulis tertarik untuk melakukan penelitian bagaimana menerapkan algoritma *blowfish* dalam pada *watermarking* video digital.

## 2. TEORITIS

### 2.1 Kriptografi

Kriptografi adalah ilmu mengenai teknik enkripsi dimana "naskah asli" (*plaintext*) diacak menggunakan suatu kunci enkripsi menjadi "naskah acak yang sulit dibaca" (*ciphertext*) oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli. Probabilitas mendapat kembali naskah asli oleh seseorang yang tidak mempunyai kunci dekripsi dalam waktu yang tidak terlalu lama

adalah sangat kecil. Teknik enkripsi yang digunakan dalam kriptografi klasik adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk public key cryptography, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan – bilangan yang sangat besar[2].

### 2.2 Watermarking

*Watermarking* adalah proses penambahan kode identifikasi secara permanen ke dalam data digital. Kode identifikasi tersebut dapat berupa teks, suara, gambar, atau video. Selain tidak merusak data digital yang dilindungi, kode identifikasi seharusnya memiliki ketahan/*robustness* terhadap berbagai pemrosesan lanjutan seperti pengubahan, kompresi, enkripsi, dan lain sebagainya. *Watermarking* merupakan aplikasi dari steganografi, namun ada perbedaan antara keduanya. Jika pada steganografi informasi rahasia disembunyikan di dalam media digital dimana media penampung tidak berarti apa-apa, maka pada *watermarking* justru media digital tersebut yang akan dilindungi kepemilikannya dengan pemberian label hak cipta atau *watermark*[3][6].

### 2.3 Algoritma Blowfish

Blowfish merupakan algoritma kunci simetrik cipher blok yang dirancang pada tahun 1993 oleh Bruce Schneier untuk menggantikan DES. Pada saat itu banyak sekali rancangan algoritme yang ditawarkan, namun hampir semua terhalang oleh paten atau kerahasiaan pemerintah Amerika. Schneier menyatakan bahwa blowfish bebas paten dan akan berada pada domain publik. Dengan pernyataan Schneier tersebut blowfish telah mendapatkan tempat di dunia kriptografi, khususnya bagi masyarakat yang membutuhkan algoritme kriptografi yang cepat, kuat, dan tidak terhalang oleh lisensi.

Keberhasilan blowfish dalam menembus pasar telah terbukti dengan diadopsinya blowfish sebagai Open Cryptography Interface (OCI) pada kernel linux versi 2.5 keatas. Dengan diadopsinya blowfish, maka telah menyatakan bahwa dunia open source menganggap blowfish adalah salah satu algoritme yang terbaik. Kesuksesan blowfish mulai memudar setelah kehadiran algoritme-algoritme dengan ukuran blok yang lebih besar, seperti AES. AES sendiri memang dirancang untuk menggantikan DES. Sehingga secara keseluruhan AES lebih unggul dari DES dan juga blowfish. [4]

### 2.3 Video Digital

Video adalah teknologi menangkap, merekam, memproses, menyimpan, dan merekonstruksi suatu urutan dari beberapa gambar. Video pertama kali dikembangkan untuk sistem televisi *cathode ray tube* (tabung sinar katode). Video digital pada dasarnya tersusun atas serangkaian *frame* yang ditampilkan dengan kecepatan tertentu (*frame* / detik). Jika laju *frame* cukup tinggi, maka mata manusia melihatnya sebagai rangkaian yang kontinu.

Masing – masing frame merupakan gambar / citra digital. Suatu gambar digital direpresentasikan dengan sebuah matriks yang masing – masing elemennya merepresentasikan nilai intensitas. Jika I adalah matriks dua dimensi, I(x,y) adalah nilai intensitas yang sesuai pada posisi baris x dan kolom y pada matriks tersebut. Titik – titik ditempat image di-sampling disebut *picture elements*,atau disebut pixel.

#### a. Resolusi/ dimensi frame

Resolusi (*resolution*) atau dimensi frame (*frame dimention*) adalah ukuran sebuah frame Resolusi dinyatakan dalam pixel x pixel .Semakin tinggi resolusi, semakin baik kualitas video tersebut, dalam arti bahwa dalam ukuran fisik sama, video dengan resolusi tinggi akan lebih detil. Namun, resolusi yang tinggi akan mengakibatkan jumlah bit yang diperlukan untuk menyimpan atau mentransmisinya meningkat.

#### b. Kedalaman Bit (bit depth)

Kedalaman bit (*bit depth*) menentukan jumlah bit yang digunakan untuk merepresentasikan tiap piksel pada sebuah frame. Kedalam bit dinyatakan dalam bit/piksel. Semakin banyak jumlah bit yang digunakan untuk merepresentasikan sebuah piksel yang berarti semakin tinggi kedalaman pikselnya, maka semakin tinggi pula kualitasnya, dan akibatnya jumlah bit yang diperlukan menjadi lebih tinggi. Dengan 1 byte (8 bit) untuk tiap piksel, level intensitas. Dengan level intensitas sebanyak itu, umumnya mata manusia sudah dapat dipuaskan. Kedalaman piksel paling rendah terdapat pada binary value image yang hanya menggunakan 1 bit untuk tiap piksel, sehingga hanya ada dua kemungkinan bagi tiap piksel, yaitu 0 (hitam) atau 1 (putih).

#### c. Laju Frame (frame rate)

Laju frame menunjukkan jumlah frame yang digambar tiap detik dan dinyatakan dengan frame/detik. Sehubungan dengan laju frame in ada dua hal yang perlu diperhatikan, yaitu kehalusan gerakan (*smooth motion*) dan kilatan (*flash*). Kehalusan gerakan ditentukan oleh frame yang berbeda per detik. Untuk mendapatkan gerakan yang halus,

video digital setidaknya harus menampilkan sedikitnya 25 frame per detik. Kilatan ditentukan oleh jumlah berapa kali layar digambar per detik, dengan 20 frame perdetik kilatan sudah dapat dilenyapkan.

**d. Representasi Warna**

Pada video digital, umumnya representasi warna video dipisahkan menjadi komponen – komponen, baik komponen warna maupun komponen kecerahan. Penyajian semacam ini disebut component video. Berberapa cara pemisahan komponen tersebut adalah RGB, YUV, YIQ. Pada RGB data video dipisahkan menjadi kompnen-komponen untuk masing-masing warna, yaitu merah(red), hijau(green), dan biru(blue). Warna tiap piksel ditentutukan oleh intensitas masing – masing komponen warna. Pada YUV pemisahan komponen tidak hanya dilakukan dengan pemisahan warna namun juga dilakukan dengan memisahakan menurut komponen kecerahan (luminance) dan komponen warna (crominance). Pada format PAL, sinyal kecerahan dinyatakan dengan Y, sedangkan dua sinya warna dinyatakan dengan U dan V. Masing-masing komponen tersebut diperoleh dengan mentransformasikan RGB dengan rumus :

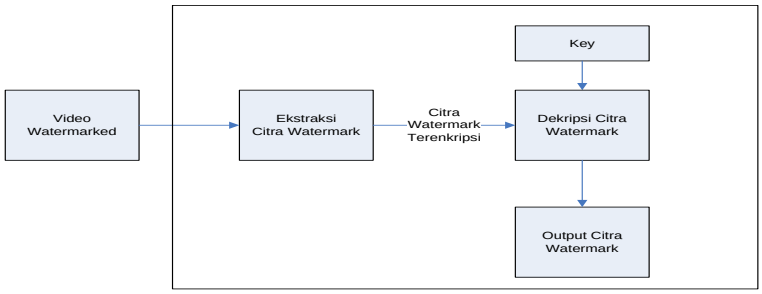
Y = 0,299 R + 0,587 G + 0,144 B
U = (B-Y) x 0,493
V = (R-Y) x 0,877

Pada YIQ pemisahan sinyal video menjadi komponen kecerahan dan komponen warna dilakukan dengan format NTSC, komponen kecerahan dinyatakan dengan Y, dan komponen warna dinyatakan dengan I dan Q. Masing – masing komponen tersebut diperoleh dengan mentransformasikan RGB dengan rumus :

Y = 0,299 R + 0,587 G + 0,114 B
I = 0,596 R – 0,257 G – 0,321 B
Q = 0,212 R – 0,532 G – 0,311 B

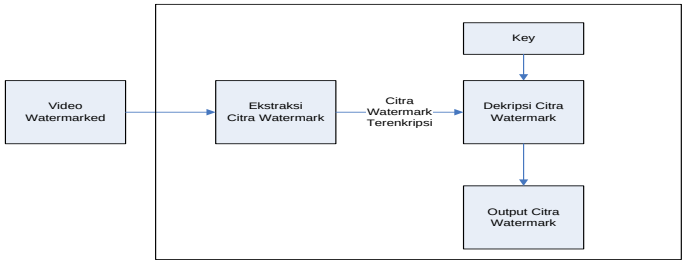
## 3. ANALISA DAN PEMBAHASAN

Pada tahap ini akan ditampilkan hasil implementasi dari algoritma *blowfish* pada watermarking video digital menggunakan aplikasi VB.Net. Namun sebelumnya akan dibahas tentang blok diagram proses watermarking.




Gambar 1. Blok Diagram Proses Embedding Watermark

Proses sistem watermarking diawali dengan melakukan enkripsi blowfish pada input citra watermark yang akan di sisipkan ke dalam video tujuan. Kunci yang digunakan adalah kunci yang ditentukan oleh pengguna. Bit data hasil enkripsi dari citra watermark kemudian akan disisipkan pada video tujuan pada setiap frame dari video yang kemudian akan dihasilkan dalam bentuk video keluaran yang telah mengandung citra watermark ter-enkripsi beserta informasi tambahan seperti ukuran citra, sebaran bit citra, dan flag penanda.




Gambar 2. Blok Diagram Proses Ekstraksi Watermark

Deteksi watermark dari video yang dibuka diawali dengan membaca bit – bit data citra watermark yang terenkripsi pada setiap frame video. Bit – bit data yang di ekstraksi kemudian akan di dekripsi menggunakan metode blowfish dengan kunci yang sama dengan saat proses dekripsi. Hasil dekripsi kemudian akan ditampilkan berupa citra watermark yang terkandung di dalam video yang dibuka. Jika ternyata video tidak mengandung watermark sama sekali sistem akan mendeteksi flag penanda yang telah ditanamkan pada video. Jika video tidak memiliki flag penanda maka video tersebut tidak mengandung citra watermark.

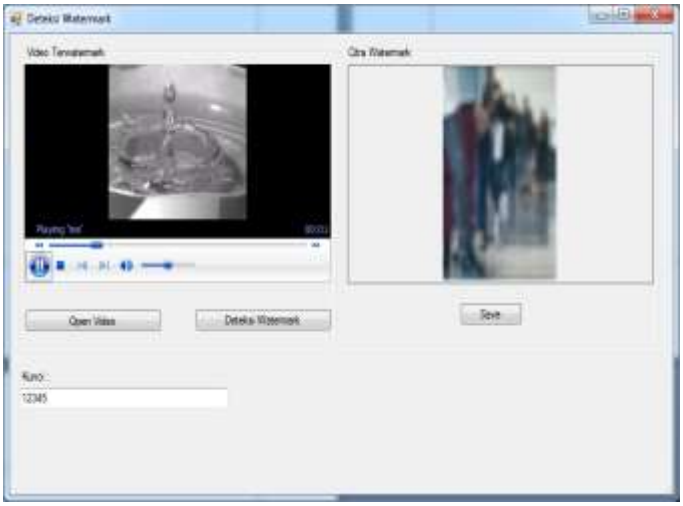
Dari blok diagram yang telah dijelaskan berikut hasil implementasi dari algoritma *blowfish* pada watermarking video digital menggunakan aplikasi VB.Net.


Gambar 3. Tampilan Awal Program

Gambar 3 menjelaskan proses untuk melakukan watermarking video digital, proses validasi watermarking dan untuk keluar dari aplikasi.


Gambar 4. Tampilan Proses Watermark Menggunakan Algoritma Blowfish

Gambar 4 menjelaskan bagaimana proses video digital diwatermark menggunakan algoritma *blowfish*. Pada proses tersebut akan dilakukan pengenkripsian dengan memasukkan kunci yang sudah ditentukan. Hasil enkripsi itulah yang akan dijadikan watermark pada video digital.



Gambar 5. Tampilan Pendeteksian Watermark

Gambar 5 menjelaskan video digital yang sudah di watermark menggunakan algoritma *blowfish* untuk dideteksi apakah proses watermarking yang dilakukan seperti pada gambar 3.5 sudah berhasil atau belum. Jika sudah berhasil maka video tersebut dapat disimpan.

## 4. KESIMPULAN

Berdasarkan pengujian yang telah dilakukan pada watermarking video digital menggunakan metode algoritma *blowfish* dengan aplikasi VB.Net dapat disimpulkan bahwa aplikasi yang dibuat dapat diimplementasikan dengan baik untuk watermarking video digital. Tingkat keamanan untuk watermarking juga sangat aman dikarenakan adanya metode algoritma *blowfish*. Namun untuk kunci dari algoritma *blowfish* sebaiknya digunakan lebih panjang. Diharapakan pula ke depannya penelitian ini dapat dikembangkan denga metode yang lebih baik atau dikombinasikan dengan metode lain.

## REFERENCES

[1] Utami, E & Aryani, S., E. 2010. Penerapan Algoritma *Blowfish* Untuk Membuat Sebuah Model Kriptosistem Algoritma dan Menganalisis Kinerja Algoritma *Blowfish* dengan Simulasi Data Terbatas. Jurnal DASI**11**(2): 33-44.
[2] Kromodimoeljo, Sentot. 2010. Teori dan Aplikasi Kriptografi. SPK IT Consulting.
[3] Septianingsih, R. 2012. Implementasi Watermarking pada Citra Digital Menggunakan Metode LSB. Skripsi.
[4] Wardoyo, Siswo,.dkk. 2016. Enkripsi dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android. DOI : 10.20449/jnte.v5il.199.
[5] Yonata, Yosi. 2002. Kompresi Video : singkat, padat, jelas. Jakarta: Elex Media Komputindo.
[6] M. Mesran, APLIKASI PENGAMANAN DATA TEKS PADA CITRA BITMAP DENGAN MENERAPKAN METODE LEAST SIGNIFICANT BIT (LSB), Pelita Inform. Inf. Dan Inform. 2 (2012).