Jurnal Teknologi dan Rekayasa Manufaktur

JTRM | Vol. 3 | No. 2 | Tahun 2021
ISSN (P): 2715-3908 | ISSN (E): 2715-016X
DOI: HTTPS://DOI.ORG/10.48182/jtrm.v3i2.58

Proteksi Keamanan Data pada Quick Response (QR) Code

Abdur Rahman Harits M[1], Ridwan[2], Angga Putra Hafidzin[3], Muhammad Taufik[4],

[1] Politeknik Manufaktur Bandung

Email: harits@polman-bandung.ac.id

Informasi Artikel:

Received:
11 Mei 2021

Accepted:
01 Desember 2021

Available:
15 Desember 2021

ABSTRAK

Penggunaan *Quick Response* (QR) *Code* untuk berbagi ataupun menyimpan data semakin marak digunakan. Kode QR dapat dengan cepat memberikan informasi baik kontak, *plain text*, URL ataupun data lainnya hanya dengan memindai QR menggunakan kamera *smartphone*. Meningkatnya penggunaan kode QR harus diiringi juga dengan tingkat keamanan dalam proteksi data. Jurnal ini membahas beberapa metode yang dapat digunakan untuk meningkatkan keamanan data pada kode QR. Dalam ilmu komputer dan matematika dikenal beberapa istilah terkait proteksi pesan/data yaitu Kriptografi dan Steganografi. Kriptografi akan mengubah pesan menjadi sebuah ciphertext menggunakan algoritma enkripsi dan *secret key*. Sedangkan pada Steganografi, pesan akan disembunyikan pada sebuah objek. Dengan kedua proses tersebut baik kriptografi dan steganografi ataupun kombinasi dari keduanya maka pesan/data yang disematkan pada kode QR tidak akan mudah untuk diterjemahkan. Metode yang akan dibahas yaitu enkripsi Algoritma Speck dan *Advance Encryption Standard* (AES) dengan kombinasi Steganografi. Kedua metode tersebut berhasil mengubah informasi rahasia menjadi data yang tidak mudah dikenali. Informasi rahasia yang mengalami proses steganografi menjadi sulit dideteksi dan memberikan pesan yang salah kepada peretas.

Kata Kunci:

QR *Code*
Kriptografi
Steganografi
Algoritma Speck
Advanced Encryption Standard

ABSTRACT

The implementation of Quick Response (QR) Code to share or store information increased widely. QR code can quickly provide a data or information such as contact person, plain text, URLs or other data by scan a QR code using smartphone camera. The raised of QR code implementation must to be follow by a level of data security. In this journal we will discuss a number of processes that can be used to improve data security in QR codes. In computer science there are several terms related to data protection i.e. Cryptography and Steganography. Cryptography focuses on securing information in the data exchange process. Steganography is a process of hiding information into an object that cannot be detected by anyone without a steganographic key. With these two processes i.e. cryptography and steganography or a combination of both, the data embedded in the QR code will not be easy to translate. The method that will be discussed is Speck Algorithm encryption and Advanced Encryption Standard (AES) with a combination of Steganography. Both methods succeed in converting confidential information into data that is not easily recognized. Confidential information that goes through a steganographic process becomes difficult to detect and gives the wrong message to a third party.

1 PENDAHULUAN

Teknik Kriptografi, Steganografi dan Watermarking dapat digunakan untuk memperoleh keamanan,kerahasiaan, privasi, dan keaslian data [1]. Kriptografi mengenkripsi pesan dan membuatnya bentuk yang tidak dapat dibaca yang disebut cipher. Sedangkan steganografi menyembunyikan data dalam media seperti file teks, gambar, audio, video dll, dan menyembunyikan keberadaan pesan dalam media. Kriptografi merupakan salah satu bidang ilmu komputer dan matematika yang berfokus pada pengamanan informasi dalam proses pertukaran data [4]. Informasi yang akan dikirim kepada penerima terlebih dahulu mengalami proses enkripsi, hasil dari proses enkripsi adalah sebuah *ciphertext* yang nantinya akan dikirim kepada penerima. Untuk mendapatkan informasi sesungguhnya dari sebuah *ciphertext,* penerima harus melakukan proses dekripsi sesuai dengan parameter *secret key* dan algoritma enkripsi yang digunakan. Sehingga apabila dalam proses transmisi terdapat pihak ketiga yang mencoba mengambil data tersebut, maka data yang ditampilkan bukanlah informasi yang sesungguhnya.

Steganografi adalah proses penyembunyian informasi ke sebuah objek yang tidak dapat diketahui oleh siapapun tanpa adanya *steganographic key* [5]. Berbeda dengan kriptografi yang bertujuan untuk mengamankan pesan pada saat transmisi, steganografi lebih mengarah pada penyembunyian keberadaan pesan itu sendiri [6]. Perkembangan steganografi dilandasi karena adanya kelemahan pada sistem enkripsi [2]. Steganografi dapat diimplementasikan untuk bertukar informasi rahasia tanpa diketahui, tidak seperti enkripsi yang membuat *ciphertext* dapat dideteksi keberadaannya dan juga rentan terhadap penyadapan.

Kode Quick Respon (QR) adalah kode batang dua dimensi yang mampu mengkodekan berbagai jenis data seperti biner, numerik, alfanumerik sebagai citra digital [1] [2].Penggunaan QR *code* sebagai media penyimpanan data saat ini semakin meningkat seiring dengan penggunaan perangkat mobile berbasis kamera dan koneksi internet. Untuk mendapatkan informasi dalam sebuah *QR code*, pengguna perlu memindai *QR code* menggunakan pemindai tertentu seperti kamera smarphone. Pemindaian QR *code* dapat dilakukan dengan cepat dikarenakan terdapat *item* pada struktur QR *code* yang mampu memberikan acuan pada kamera terkait orientasi objek sehingga informasi dapat diterjemahkan oleh kamera walaupun sudut pembacaan objek dua dimensi tidak begitu baik [3].

Penggunaan QR *code* sudah banyak diterapkan diberbagai macam industri seperti *Food & Beverages, Automotive, Manufacture* dan sektor lainnya. Penerapan QR *code* pada produk *Food & Beverage* bertujuan untuk menghubungkan konsumen dengan produsen [3]. Konsumen dapat mengetahui seluruh informasi terkait produk dari awal produksi, informasi kualitas bahan, uji sertifikasi sampai pendistribusian produk ke toko retail. Tentunya penerapan QR *code* pada setiap sektor industri memiliki kegunaan dan karakteristiknya masing-masing. Selain itu tidak jarang juga dijumpai QR *code* pada kegiatan jual beli sebuah produk, seperti klaim kupon potongan harga ataupun hanya sekedar *online payment*. Mengingat betapa pentingnya privasi data terhadap kegiatan yang mengimplementasikan QR *code,* maka perlu dilakukannya proteksi data baik dengan proses kriptografi ataupun steganografi.

Upaya meningkatkan keamanan data pada QR *code* dapat dilakukan dengan proses kriptografi dan steganografi ataupun kombinasi dari keduanya. Pada bagian 2 jurnal ini akan membahas penelitian terkait struktur QR *code,* kriptografi dan steganografi. Pada bagian 3 menjelaskan metode kriptografi menggunakan algoritma *speck* dan juga metode steganografi pada pesan yang sudah terenkripsi. Pada bagian 4 membahas hasil analisis dari

kedua metode sebelumnya. Pada bagian 5 berisi kesimpulan terkait upaya proteksi data pada QR *code.*

2 PENELITIAN TERKAIT

2.1 Struktur QR Code

QR *code* memiliki struktur dalam penyematan data. Struktur tersebut terdiri dari beberapa item yang memiliki fungsi masing-masing, pada Gambar 1 merupakan struktur QR *code* yang terdiri dari 7 itemd dengan penjelasan sebagai berikut [7]:

Gambar 1. Struktur QR Code

1. *Finder Pattern*
    Merupakan pola dari struktur QR code yang berfungsi untuk identifikasi posisi. Dengan adanya finding pattern ini, pemindaian QR code dapat dilakukan dalam berbagai arah (sudut pembacaan 360^0).
2. *Format Information*
    Merupakan informasi yang berisi *error correction level* dan *mask pattern* dari QR *code.*
3. *Timing Pattern*
    lerupakan pola struktur yang merepresentasikan koordinat pusat dari QR *code,* ditandai dengan pola bergantian hitam dan putih.
4. *Version Information*
    Merupakan struktur yang merepresentasikan versi QR *code* yang digunakan (mulai dari versi 1 hingga 40). Versi QR *code* yang digunakan menentukan jumlah sel dan konfigurasinya.
5. *Alignment*
    Merupakan pola dari struktur yang memberikan acuan terkait kesejajaran pemindaian QR *code*, berguna juga pada saat terjadi distorsi non-linear.
6. *Data*
    Merupakan bagian dari struktur QR *code* berupa sel hitam dan putih yang merepresentasikan informasi rahasia.
7. *Quiet zone*
    Bagian terluar dan area kosong dari QR *code* yang mempermudah pemindaian informasi.

Mona dan Jethava [8] menyampaikan metode untuk mengurangi kapasitas penyimpanan data dari QR *code* yang sudah diexport menjadi gamba sehingga akan banyak informasi yang dapat disematkan ke dalam sebuah QR *code*. Metoda kompresi yang digunakan yaitu *Zip Compression Algorithm*, dengan melakukan kompresi maka data akan tersimpan secara efisien, mengurangi *transmission cost* dan *transmission time*. Mula-mula data yang akan disematkan terlebih dahulu dibuah kedalam bentuk ASCII, lalu bentuk ASCII tersebut diubah

kedalam biner dan dilakukan proses kompresi dengan *Zip Compression Algorithm*. Data hasil kompresi dibuat menjadi sebuah QR *code* dan dilakukan *multiplexing/*pengandaan menjadi 5 bagian. Setelah itu dilakukan pengambilan bit tunggal dari masing-masing 5 kode QR, sehingga kombinasi terbentuk sebuah QR *code*. 5 bit data pengelompokan akan diganti oleh masing-masing karakter/simbol khusus seperti pada tabel 1 bawah ini:

Tabel 1. Pemetaan 5 Bit Symbol

Module in each pattern	Symbol	Module in Each Pattern	Symbol	Module in Each Pattern	Symbol
00000	!	01011	/	10011	?
00001	#	01100	.	11000	L
00010	$	01101	,	11001	_
00011	%	01110	:	11110	}
00100	&	01111	;	10100	@
00101	"	10000	<	10101	\
00110	(	10001	>	11010	[
00111	)	10110	V	11011	]
01000	+	10111	^	11111	`
01001	-	11100	M		
01010	*	11101	{		

QR *code* yang dihasilkan memiliki kapasitas penyimpanan data yang lebih kecil dari sebelumnya yaitu 3KB menjadi 1KB. Dimana mereka juga membandingkan hasil kompresi dengan algoritma Huffman Compression yaitu 1.2KB.

2.2 Kriptografi

Rahmanita dan Erni [9] menyampaikan solusi keamanan data pada QR code dengan metode enkripsi Vigenere Cipher. Vigenere Cipher merupakan pengembangan dari enkripsi Caesar Cipher dimana dasar dari algoritma ini adalah beberapa huruf dari kata kunci diambil dari pergeseran yang dilakukan oleh Caesar Cipher. Algoritma enkripsi ini dapat dilakukan dengan menggunakan substitusi angka maupun bujursangkar vigenere.

Calvin dan Prasetyo [10] [11] menyampaikan penerapan QR *code* dengan algoritma enkripsi RSA pada tiket masuk festival. RSA merupakan algoritma penyandian informasi menggunakan dua kunci yang berbeda yaitu untuk enkripsi dan dekripsi. Tingkat keamanan algoritma RSA bergantung pada ukuran kunci sandi tersebut (dalam bentuk bit). Dalam proses algoritma RSA, terdapat cara tersendiri untuk menciptakan kunci baik bersifat privat maupun publik. Berikut ini adalah cara untuk membuat kunci pada penyandian RSA:

1. Pilih dua bilangan prima untuk *p* dan *q* secara acak, dimana $p \neq q$.
2. Hitung nilai $N = pq$, sebagai parameter keamanan.
3. Hitung nilai $\varphi = (p-1)(q-1)$, sebagai nilai untuk menentukan *e.*
4. Tentukan nilai *e,* dimana $\varphi < e < N$. Nilai *e* bersifat bilangan prima dan merupakan bilangan bulat.
5. Hitung *d* hingga $d\,e \equiv 1 \pmod{\varphi}$.

Proses enkripsi dapat diselesaikan dengan menggunakan metode *exponentiation by squaring*, yaitu sebuah algoritma yang dipakai untuk komputasi terhadap sejumlah nilai integer yang besar dengan cepat. *Ciphertext* yaang sudah didapatkan menjadi informasi

yang akan disematkan pada QR *code.* Berikut ini adalah rumus enkripsi RSA pada persamaan (1):

$$c = n^e \, Mod \, N \qquad (1)$$

Pembacaan QR *code* dilakukan dengan metode dekripsi algoritma RSA dan memerlukan kunci dekripsi yaitu *d*. Dibawah terdapat persamaan (2) yang merupakan rumus dekripsi pada algoritma RSA:

$$n = c^d \, Mod \, N \qquad (2)$$

2.3 Steganografi

Munir Rinaldi [12] menyampaikan bahwa steganografi adalah ilmu dan seni menyembunyikan informasi pada suatu dengan mengubah bit informasi ke dalam file host (media penampung) dan data file tersebut tampak biasa, bukan rahasia dengan tingkat distorsi tanpa mempengaruhi kualitasnya sehingga keberadaan/eksistensi pesan tidak terdeteksi. Steganografi terdiri dari dua bagian yaitu media penampung dan informasi yang akan disembunyikan. Pada Steganografi digital menggunakan media digital sebagai media penampung, misalnya citra digital, audio digital, dan video digital. Pesan rahasia yang disembunyikan juga berbentuk digital, seperti file citra, audio, teks, dan video.

Menurut Ariyus [13] pada jurnal keamanan multimedia, ada tujuh teknik dasar yang digunakan dalam steganografi, yaitu:

1. Injection, merupakan suatu teknik menyisipkan informasi/pesan rahasia secara langsung ke suatu media. Salah satu masalah dari teknik ini adalah ukuran media yang disisipkan menjadi lebih besar dari ukuran normalnya sehingga informasi mudah dideteksi. Teknik ini sering juga disebut embedding.
2. Substitusi, adalah teknik menyembunyikan data dengan menggantikan data normal ke data rahasia. Biasanya, hasil teknik ini tidak terlalu mengubah ukuran media, tetapi pada teknik substitusi bisa menurunkan kualitas media yang ditumpangi.
3. Transform Domain merupakan suatu teknik menyembunyikan data pada transform space ke dalam suatu media. Media yang efektif pada tekni ini adalah file berekstensi JPG.
4. Spread Spectrum, sebuah teknik pengiriman data dengan menggunakan pseudo-noise code, yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (bandwidth) yang lebih besar daripada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika pseudo-noise code tersinkronisasi.
5. Statistical Method, adalah teknik skema steganographic 1 bit. Dimana skema tersebut berisi informasi pada embedded message dan mengubah statistik walaupun hanya 1 bit. Sistem ini bekerja berdasarkan kemampuan penerima dalam membedakan antara informasi yang dimodifikasi dan yang belum.
6. Distortion, metode ini membuat perubahan atas media yang ditumpangi oleh data rahasia sehingga sulit terdeteksi oleh indera manusia
7. Cover Generation, metode ini lebih unik daripada metode lainnya karena cover object dipilih untuk menyembunyikan pesan.

3 METODE PROTEKSI DATA

Dewasa ini metode yang digunakan untuk meningkatkan keamanan data banyak diteliti dan dipelajari dari berbagai aspek. Pada jurnal ini kami akan membahas tentang metode proteksi data pada QR *code* yaitu enkripsi algoritma speck dan steganografi dengan kombinasi algoritma *Advanced Encryption Standard* (AES).

3.1 Algoritma Speck

Algoritma Speck adalah salah satu algoritma *Lightweight block cipher* guna memenuhi kebutuhan suatu metode penyandian pada suatu media dengan sumber daya yang sangat terbatas, seperti memori, daya komputasi dan pasokan baterai [14]. Kriptografi Lightweight (ringan) adalah kriptografi ringan yang telah menjadi topik tren untuk beberapa tahun terakhir ini dan munculnya kriptografi ini didorong oleh kurangnya aplikasi yang mampu berjalan pada perangkat berdaya komputasi yang sangat rendah [15]. Algoritma Speck diajukan oleh peneliti yang bekerja pada *National Security Agency* (NSA) di Amerika. Pemetaan acak adalah persyaratan yang harus dimiliki suatu algoritma *block cipher*. Terdapat 10 varian dari algoritma Speck berdasarkan panjang kunci dan ukuran blok pesannya seperti dapat dilihat pada tabel 2. Berikut notasi (gambar 2) yang digunakan pada algoritma speck:

Tabel 2. Varian dan Parameter Algoritma Speck

Block size 2n	Key size mn	Word size n	Key words m	Rot α	Rot β	Rounds r
32	64	16	4	7	2	22
48	72	24	3	8	3	22
48	96	24	4			23
64	96	32	3	8	3	26
64	128	32	4			27
96	96	48	2	8	3	28
96	144	48	3			29
128	128	64	2	8	3	32
128	192	64	3			33
128	256	64	4			34

Notasi Algoritma Speck adalah sebagai berikut :

Ɵ : operator bitwise XOR
n : Ukuran panjang word pada speck (n=16,24,32,48 atau 64)
+ : operator penjumlahan modulo 2n
- : Operator Pengurangan modulo 2n
<< j : Rotasi bit ke kiri sebanyak j bit
>> j : Rotasi bit ke k sebanyak j bit
r : Jumlah round
a<- b : memperbarui nilai a dengan b

Pada algoritma speck terdapat 3 proses utama yang harus dilakukan yaitu enkripsi, pembangkitan kunci dan dekripsi. Berikut ini adalah penjelasan singkat mengenai ketiga proses tersebut:

1. Enkripsi
   Proses enkripsi pada algoritma speck menggunakan kunci yang diterapkan pada key ekspansi [14]. Berikut ini adalah gambar 3 yang menjelaskan proses enkripsi algoritma speck:

Proses Enkripsi Algoritma Speck
Input : $X_{(2n)};\ K_0, \dots, K_{r-1}$
Output :$Y_{(2n)}$

Proses :

1. $X_{0(n)}|X_{1(n)} \leftarrow X_{(2n)}$
2. $untuk\ i = 1\ sampai\ dengan\ r-1$

$$X_1 \leftarrow \big((X_1 \gg \alpha) + X_0\big) \oplus k_i$$
$$X_0 \leftarrow ((X_0 \gg \beta)) \oplus X_1$$

3. Output :

$$Y_{(2n)} \leftarrow X_{0(n)}|X_{1(n)}$$

a. Menguraikan nilai $X_{(2n)}$ menjadi $X_{0(n)}|X_{1(n)}$.
b. Memperbarui nilai X_1 menjadi nilai X_1 yang telah digeser ke kanan sejauh α bit dan dilakukan operasi penjumlahan modulo X_0 serta operasi XOR dengan k_i.
c. Memperbarui nilai X_0 menjadi nilai X_0 yang telah digeser ke kanan sejauh β bit dan operasi XOR dengan X_1.
d. Memperbarui nilai $Y_{(2n)}$ menjadi nilai $X_{0(n)}|X_{1(n)}$.

Hasil dari enkripsi menggunakan algoritma speck akan disandikan sebagai informasi yang tersemat pada QR *code*. Sehingga informasi apabila dilakukan proses pemindaian maka akan memunculkan *ciphertext* yang tidak mudah untuk diterjemahkan. Agar dapat membaca *ciphertext* yang disematkan perlu adanya proses dekripsi menggunakan algoritma speck tentunya.

2. *Key Schedule* (Pembangkitan Kunci)
Pada dasarnya proses pembangkitan kunci algoritma speck masih menggunakan kunci yang sama seperti proses enkripsinya akan tetapi kunci tersebut diganti menjadi nilai *rounds* [14]. Parameter yang digunakan untuk proses pembangkitan kunci ada 2 yaitu k_i dan l_i. Lalu bagaimanakah cara untuk mendapatkan parameter l_i yang belum diketahui, berikut ini adalah persamaan (3) yang digunakan [16]:

$$l_{i+m-2} \leftarrow (k_i + (l_i \gg \alpha)) \oplus i \qquad (3)$$

Parameter m merupakan key words sesuai dengan jenis speck yang dipakai (lihat pada tabel 2). Nilai i merupakan angka siklus dari 0 sampai dengan r-1 dimana r adalah round yang ada pada tabel 2. Setiap akhir dari siklus maka nilai i akan bertambah 1. Berikut penjelasan singkat pada proses pembangkitan kunci:

a. Lakukan pergeseran bit ke kanan sejauh ɑ pada li.
b. Operasi penjumlahan modulo 2n antara ki dan li yang sudah dilakukan pergerseran.
c. Setelah itu lakukan operasi *bitwise XOR.*
d. Memperbarui nilai $li + m$ dengan hasil operasi pada bagian sebelumnya.

Berikut ini adalah rumus persamaan (4) yang digunakan untuk membangkitkan kunci:

$$K_{i+1} \leftarrow (K_i \ll \beta) \oplus l_{i+m-2} \qquad (4)$$

a. Lakukan operasi pergeseran bit ke kiri sejauh β pada k_i
b. Hasil dari operasi geser dilakukan operasi *bitwise XOR* dengan l_{i+m-2} yang sudah didapatkan pada proses sebelumnya.
c. Memperbarui nilai k_{i+1} dengan hasil operasi keseluruhan.

3. Dekripsi
Proses untuk melakukan dekripsi pada algoritma speck memerlukan invers operasi modulo, proses putaran sama dengan enkripsi, perbedaannya pelibatan key ekspansi

dalam prosesnya dibalik dari indek akhir sampai ke awal. Berikut ini gambar 4 yang memperlihatkan proses dekripsi pada algoritma speck:

Proses Dekripsi Algoritma Speck

Input : $Y_{(2n)}; k_0, \dots, k_{r-1}$

Output : $X_{(2n)}$

Proses :

1. $Y_{0(n)}|Y_{1(n)} \leftarrow Y_{(2n)}$
2. Untuk $i = 1$ sampai dengan $r - 1$
   $Y_0 \leftarrow (Y_0 \oplus Y_1) \gg \beta$
   $Y_1 \leftarrow \left((Y_1 \oplus k_{r-i-1}) - Y_0\right) \ll \alpha$
3. *Output* :
   $X_{(2n)} \leftarrow Y_{0(n)}|Y_{1(n)}$

Proses Dekripsi Algoritma Speck

Input : $Y;\ K_0, \dots, K_{r-1}$
Output :$X_{(2n)}$
Proses :
1. $Y_{0(n)}|Y_{1(n)} \leftarrow Y_{(2n)}$
2. $untuk\ i = 1\ sampai\ dengan\ r - 1$

$$Y_0 \leftarrow (Y_0 \oplus Y_1) \gg \beta$$
$$Y_1 \leftarrow ((Y_1 \oplus k_{r-i-1}) - Y_0) \ll \alpha$$

Output :

$$X_{(2n)} \leftarrow Y_{0(n)}|Y_{1(n)}$$

a. Menguraikan $Y_{(2n)}$ menjadi $Y_{0(n)}|Y_{1(n)}$
b. Lakukan operasi *bitwise XOR* antara Y_0 dan Y_1, setelah itu lakukan pergeseran bit ke kanan sejauh β serta perbarui nilai Y_0
c. Lakukan operaso *bitwise XOR* antara Y_1 dan K_{r-2}, setelah itu lakukan pergeseran bit ke kiri sebesar α serta perbarui nilai Y_1.
d. Perbarui nilai $X_{(2n)}$ dengan $Y_{0(n)}|Y_{1(n)}$.

Pesan yang sudah dipindai pada QR *code* menggunakan kamera *smartphone* dapat diterjemahkan dengan proses dekripsi. Sehingga keamanan informasi dapat terjaga dengan baik.

3.2 *Advanced Encryption Standard* dan Steganografi

Advanced Encryption Standard (AES) merupakan sebuah symmetric block cipher yang digunakan untuk melindungi informasi rahasia. Saat ini AES banyak diimplementasikan pada perangkat keras dan perangkat lunak untuk mengenkripsi data-data penting berbagai negara di dunia [17]. Diterapkan pada komputer dan perangkat lunak milik pemerintah untuk keamanan siber dan perlindungan data elektronik. Terdapat 3 versi dari AES, dimana klasifikasi tersebut didasarkan pada panjang kunci yang digunakan untuk enkripsi dan dekripsi data yaitu AES-128, AES-192 dan AES-256.

Tabel 3. Versi AES

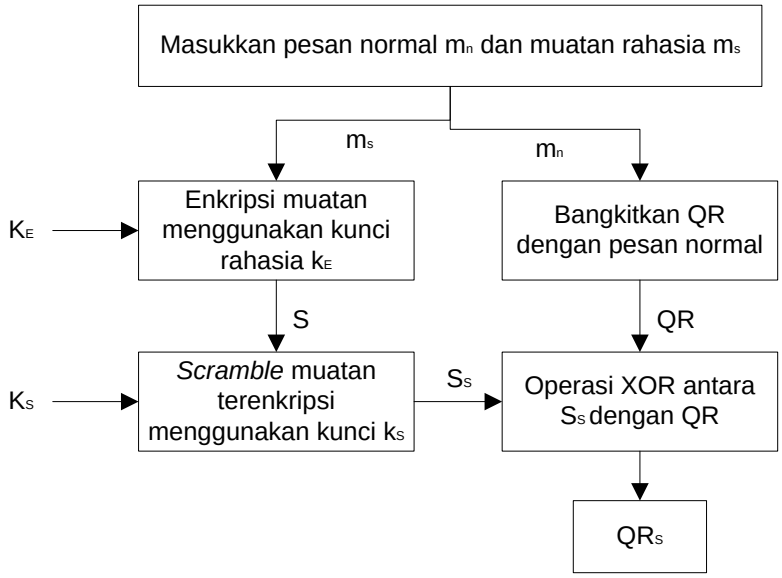
	Panjang Kunci (Nk words)	**Ukuran Blok (Nb words)**	**Jumlah Putaran (Nr)**

AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

AES pada dasarnya adalah operasi subtitusi dan permutasi yang berjalan dengan cepat pada perangkat keras dan perangkat lunak [4]. Selain permutasi dan subtitusi terdapat operasi lain di dalamnya yaitu putaran *cipher* berulang dengan kunci internal yang berbeda-beda (disebut *round key*). Berikut ini adalah alur enkripsi pada AES [18]:

1. *Add Round Key*
   Operasi *bitwise XOR* antara *initial state* (*plaintext*) dengan *cipher key.*
2. Putaran $Nr - 1$
   Proses yang terjadi pada setiap putaran adalah sebagai berikut:
   a. *Sub bytes*, Subtitusi byte dengan menggunakan tabel subtitusi.
   b. *Shift Rows,* pergeseran baris-baris *array state* secara *wrapping*.
   c. *Mix Column,* mengacak data di masing-masing kolom array state.
   d. *Add Round Key,* operasi *bitwise XOR* antara state saat ini dengan *round key.*
3. Final round
   Proses untuk putaran terakhir yang terjadi adalah sebagai berikut:
   a. *Sub bytes*, Subtitusi byte dengan menggunakan tabel subtitusi.
   b. *Shift Rows,* pergeseran baris-baris *array state* secara *wrapping*.
   c. *Add Round Key,* operasi *bitwise XOR* antara state saat ini dengan *round key.*

Proses enkripsi menggunakan algoritma AES ini merupakan bagian dari sebuah sistem yang digunakan untuk proses steganografi pesan terenkripsi ke dalam QR *code*. Berikut ini adalah gambar 5 yang memperlihatkan alur sistemnya yang digunakan [2]:



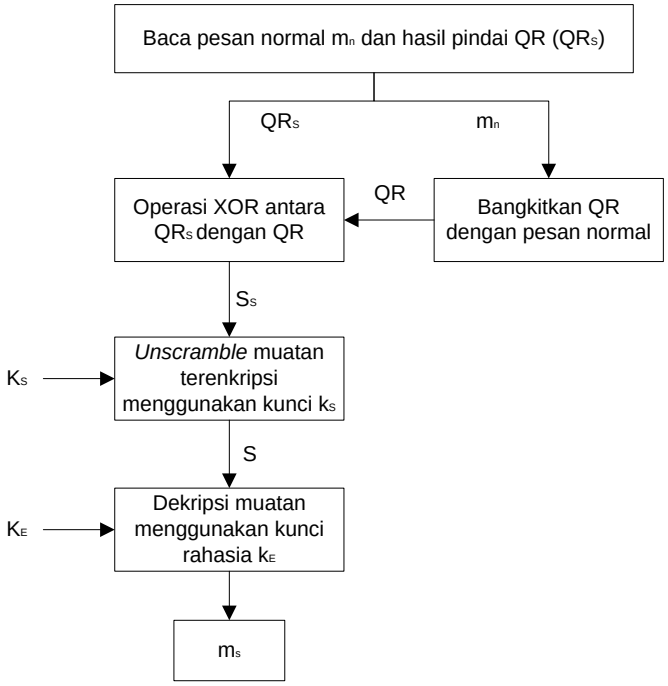
Gambar 5. Alur Sistem Steganografi Pesan Enkripsi

1. Tentukan pesan normal (m_n) dan muatan rahasia (m_s) yang akan disematkan ke dalam QR *code*.
2. Lakukan proses enkripsi pada muatan menggunakan algoritma *Advanced Encryption Standard* (AES) dengan kunci public untuk enkripsi (K_E). Muatan yang sudah ternkripsi

disebut *ciphertext* (S). Di saat yang bersamaan lakukan pembangkitan QR terhadap pesan norma.l

3. Lakukan proses *scrambling* pada *ciphertext* (S) menggunakan algoritma Baker Map dan Tent Map dengan kunci scramble (K_S) untuk mendapatkan parameter *subscript for scrambling* (S_S).
4. Lakukan operasi *bitwise XOR* antara S_S dengan QR sehingga menghasilkan kode QR yang tersemat muatan rahasia (QR_S).

Proses ekstraksi atau dekripsi muatan rahasia yang tersemat pada QR_S dilakukan dengan membalik alur sistemnya saja seperti gambar 6 berikut ini:



Gambar 6. Alur Sistem Steganografi Pesan Dekripsi

1. Scan QR untuk mendapatkan pesan normal (m_n) dan kode QR yang tersemat (QR_S).
2. Lakukan operasi *bitwise XOR* antara QR_S dengan QR sehingga menghasilkan S_S.
3. Lakukan proses *unscrambling* pada S_S menggunakan algoritma Baker Map dan Tent Map dengan kunci scramble (K_S) untuk mendapatkan *ciphertext* (S).
4. Lakukan dekripsi *ciphertext* dengan K_E untuk menghasilkan muatan rahasia (m_s).

Pada penelitian ini dilakukan pengujian sistem dengan parameter sebagai berikut:

- Pesan berisi "The meeting at 6 p.m"
- Konversi pesan ke dalam bentuk ASCII "84 104 101 32 109 101 101 116 105 110 103 32 105 115 32 97 116 32 54 32 112 46 109 46"
- Muatan rahasia berisi "The message is a decoy!. The appointment is at 3 p.m."
- Konversi muatan rahasia ke dalam ASCII "84 104 101 32 110 111 114 109 97 108 32 109 101 115 115 97 103 101 32 105 115 32 97 32 100 101 99 111 121 33 46 32 84 104 101 32 97 112 112 111 105 110 116 109 101 110 116 32 105 115 32 97 116 32 51 32 112 46 109 46"

Dengan parameter tersebut terbentuklah *generated* QR *code* dan *ordinary* QR *code,* seperti pada gambar 7 dan 8. Dapat dilihat dari kedua QR code tidak ditemukan perbedaan yang signifikan. Pemindaian kedua QR *code* pun menghasilkan data yang sama apabila dipindai dengan aplikasi QR Scanner biasa.

Gambar 7. Generated QR Code

Gambar 8. Ordinary QR Code

4 ANALISA METODE

Terdapat 2 metode proteksi data pada QR *code* yang sudah dibahas pada bagian sebelumnya yaitu algoritma speck dan steganografi dengan algoritma enkripsi AES. Berdasarkan kedua penelitian tersebut kami menganalisa bahwa masing-masing metode memiliki karakterisitik dan tujuan yang berbeda. Kesamaannya adalah kedua metode mampu mengubah informasi rahasia menjadi pesan yang tidak mudah untuk diterjemahkan, akan tetapi informasi rahasia yang melalui proses steganografi lebih sulit dikenali/dideteksi. Begitu pula dengan parameter panjang *secret key* dari kedua metode, pada algoritma *speck* memiliki panjang kunci maksimum yaitu 128-bit dan minimum 32-bit sedangkan AES memiliki panjang maksimum 256-bit dan minimum 128-bit. Dengan parameter panjang kunci kita dapat mengetahui seberapa kombinasi kunci yang dapat dibentuk, maka semakin panjang kuncinya akan semakin tangguh dalam menahan serangan *exhaustive key search*. Namun walaupun begitu algoritma *speck* dapat bekerja dengan konsumsi daya yang rendah dalam mengamankan datanya. Sedangkan tujuan dari steganografi dan kombinasi enkripsi AES adalah untuk mengecoh penyadap dalam menerjemahkan informasi rahasia. Hal tersebut terjadi karena muatan rahasia terlindungi oleh pesan normal dari QR *code*.

Penerapan QR *code* dengan algoritma speck dapat diterapkan untuk perangkat elektronik yang memerlukan konsumsi daya rendah seperti *dynamic* QR *code* pada *stand* makanan untuk urusan *online payment*, alat buka tutup pintu rumah menggunakan QR *code*, QR *code scanner* yang menggunakan batre agar tahan lama dan penerapan lainnya. Sedangkan penerapan QR *code* dengan steganografi dan algoritma AES dapat diimplementasikan pada dokumen-dokumen penting miliki negara, perusahaan atau instansi lainnya. Salah satu penerapan algoritma AES adalah pada kompresi 7-Zip.

5 KESIMPULAN

Setelah dilakukan penelitian dapat dismpulkan bahwa kedua metode tersebut dapat mengubah pesan rahasia menjadi data yang tidak mudah untuk dikenali. Kedua metode tersebut sama-sama memerlukan parameter seperti *secret key* atau kunci rahasia untuk dapat mengetahui pesan rahasia tersebut. Dengan penambahan proses steganografi pada

algoritma AES, pesan jadi semakin sulit untuk di deteksi keberadaannya serta apabila peretas tidak sadar akan adanya proses steganografi maka pesan yang didapatkan justru akan menyesatkan atau menipu.

6 REFERENSI

[1] M. Shanthi dan R. Euphrasia, "Data Security Through QR Code Encryption and Steganography," dalam *Advanced Computing: An International Journal (ACIJ)*, 2016.

[2] M. Alajmi, I. Elashry dan H. El-Sayed, "Steganography of Encrypted Messages Inside Valid QR Codes," dalam *IEEE Access*, 2020.

[3] G. Baralla, A. Pinna dan G. Corrias, "Ensure Traceability in European Food Supply Chain by Using a Blockchain System," dalam *IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, 2019.

[4] M. Barakat, C. Eder dan T. Hanke, An Introduction to Cryptography, Univesity of Kaiserslautern, 2018.

[5] A. Toumazis, "Steganography," 2009.

[6] M. Kharrazi, H. Sencar dan N. Memon, "Image Steganography: Concepts and Practice," dalam *Research Gate*, 2004.

[7] Ariadi, "Analisis dan Perancangan Kode Matriks Dua Dimensi Quick Response (QR) Code," 2011.

[8] M. Umaria dan Jethava, "Enhancing the data storage Capacity in QR code using Compression Algorithm and achieving security and Further data storage capacity improvement using Multiplexing," dalam *International Conference on Computational Intelligence and Communication Networks*, 2015.

[9] R. Syahdan dan E. Anitasari, "Penggunaan QR Code dengan Enkripsi Vigenere Cipher dalam Pengamanan Data," dalam *SEMINAR MATEMATIKA DAN PENDIDIKAN MATEMATIKA UNY*, 2017.

[10] C. Irawan, "Enkripsi Pada QR Code Tiket Dengan RSA," dalam *Institut Teknologi Bandung, Makalah IF Kriptografi*, 2010.

[11] P. A. Wicaksono, "Enkripsi Menggunakan Algoritma RSA," dalam *Institut Teknologi Bandung*, Bandung.

[12] M. Rinaldi, "Kriptografi : Steganografi dan Watermarking," 2004.

[13] A. D, "Keamanan Multimedia," 2009.

[14] E. Firmanesa dan Wildan, "Uji SAC Terhadap Algoritma Speck," 2016.

[15] A. Y. Poschmann, "Lightwight Cryptography," dalam *Unievrsity Bochum*, Bochum, 2009.

[16] Y. S. Fatmala, A. Kusyanti dan M. Data, "Implementasi Algoritme Speck untuk Enkripsi dan Dekripsi pada QR Code," dalam *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 2018.

[17] M. Rouse, "Search Security," April 2020. [Online]. [Diakses 10 May 2020].

[18] Z. Muttaqin, "Pembuatan Aplikasi Enkripsi Menggunakan Metode Advance Encryption Standard dan Rivest Shamir Adlemen," 2019.