KOMBINASI AES-PVD DALAM KRIPTOGRAFI FILE VIDEO

***Heru Pramono Hadi*[1]*, Titien S. Sukamto*[2]**
[1,2] Program Studi Sistem Infromasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Imam Bonjol 207 Semarang
e-mail: heru.pramono.hadi@dsn.dinus.ac.id, titien.suhartini@dsn.dinus.ac.id

ABSTRAK

Tidak dapat dihindari bahwa teknologi semakin maju dan memasuki era digital. Sehingga keamanan data menjadi masalah yang banyak ditemui di era ini, banyak cara dilakukan untuk mengamankan data. Beberapa cara untuk mengamankan data antara lain kriptografi dan steganografi. Salah satu algoritma dari kriptografi adalah AES. Sedangkan steganografi menyisipkan pesan ke dalam media tertentu, tetapi terlihat tidak merubah media aslinya. Media yang sering digunakan untuk steganografi adalah citra. Dalam penelitian ini, akan dilakukan pengamanan data teks yang dienkripsi dengan kriptografi AES ke dalam video dengan menggunakan steganografi PVD dan dibantu dengan algoritma LCG untuk membangkitkan bilangan acak untuk menyisipkan pesan. Dengan mengubah plainteks menjadi cipherteks, lalu disambung dengan proses penyisipan ke dalam salah satu frame di dalam video dengan menggunakan PVD, dengan hasil MSE rata-rata 3,6 dan PSNR rata-rata 43 dBs, penggabungan metode ini diharapkan dapat meningkatkan keamanan data serta dapat mengimplementasikan gabungan dari ketiga algortima tersebut.

***Kata Kunci**: AES, PVD, LCG, Video*

1. PENDAHULUAN

Keamanan data menjadi aspek yang paling penting dalam menyimpan informasi, baik informasi dalam bentuk fisik ataupun dalam bentuk digital. Zaman sekarang kita lebih menyimpan data rahasia di dalam penyimpanan cloud sejak penyimpanan itu datang ke dunia teknologi. Secara praktik, berapa banyaknya jumlah data yang akan ditransfer tidak menjadi halangan, dan yang paling penting dari semua itu adalah Channel, atau saluran yang akan kita gunakan untuk mengirimkan data, harus aman terlebih dahulu. Menurut Sari [1] Kriptografi adalah salah satu dari sekian teknik yang bertujuan untuk mengamankan transmisi data. Dan juga dengan menggunakan teknik algortima kriptografi, kita bisa menyediakan keamanan untuk informasi tersebut.

Algoritma AES adalah algoritma 128-bit blok cipher yang menggunakan ukuran kunci 128, 192, dan 256 bit. AES sebenarnya bernama Rinjdael, sesuai dengan nama pengembangnya, yang menang di dalam kompetisi yang diselenggarakan oleh NIST untuk memilih suksesor untuk penerus algoritma DES yang banyak dibobol di dalam beberapa tahun terakhir [2]. Ketika kita ingin menyimpan pesan rahasia, jika menggunakan algoritma kriptografi, banyak pihak ketiga yang akan curiga dengan pesan kitaa karena pesan kita tidak bisa dibaca secara langsung, sehingga banyak pihak tak berwenang akan berusaha untuk mengetahui pesan rahasia tersebut [3]. Maka dari itu ditemukanlah teknik penyimpanan rahasia lagi yang lebih efektif untuk menyimpan pesan, yaitu steganografi.

Steganografi didefinisikan sendiri sebagai seni untuk menyimpan informasi rahasia didalam media tertentu tanpa dapat dilihat secara langsung. Steganografi memungkinkan orang untuk berkomunikasi tanpa gangguan dari yang lain tahu tentang pesan yang ditanamkan [4]. Beberapa algoritma steganografi yang umum digunakan saat ini antara lain algoritma Least Significant Bit (LSB) [5], F5, Spread-Spectrum Image Steganography (SSIS), Pixel Value Differencing (PVD) [6], dan lain-lain. Sebuah metode untuk menanam banyak bit ke dalam beberapa pasang yang mempunyai nilai selisih piksel yang paling besar, seperti yang ditemukan di area tepi. Selisih digunakan untuk menentukan berapa banyak jumlah data yang dapat disisipkan.

Selain citra dan suara, media penyimpanan yang banyak digunakan adalah video. Video adalah image sequence, karena gambar bergerak direpresentasikan dengan urutan banyak gambar diam dengan waktu tertentu. Banyak juga penyisipan steganografi dengan citra dan suara sebagai media, tapi masih jarang ditemukan penyisipan ke dalam video. Dalam penelitian ini, akan dilakukan penyisipan pesan rahasia ke dalam video.

Beberapa penelitian sudah dilakukan, salah satunya oleh Ramadhan J. Mstafa dan Khaled M. Elleithy pada tahun 2014, dengan video yang dipecah menjadi beberapa frame sebagai tiap gambar, dan gambar tersebut dikonversi ke format YUV [7]. Dengan kualitas video dengan PSNR diatas 51 dBs, peneliti sukses menanamkan pesan rahasia di dalam video, tanpa mengurangi kualitas video tersebut. Banyak aplikasi kriptografi yang membutuhkan bilangan acak dan bilangan acak semu, contohnya untuk generate kunci kriptografi, digital signatures, dan protokol otentikasi.

Banyak algoritma kriptografi yang membutuhkan pembangkit bilangan acak seperti one time pads [8], key generation [9], Elliptic Curve Digital Signature Algorithm (ECDSA) [10] untuk mengenkripsi pusan. Urutan acak bisa dibangkitkan menjadi dua tipe pembangkit bilangan acak [11], yaitu True Random Number Generators (TRNGs) dan Psuedo-Random Number Generators (NRGs). Linear Congruential Generators (LCGs) adalah algoritma pembangkit bilangan acak bertipe PNRGs yang banyak digunakan untuk membangkitkan urutan bilangan integer acak. Keunikan dari algoritma ini adalah selalu membangkitkan bilangan yang sama apabila menggunakan parameter yang sama juga, hal ini dapat dimanfaatkan untuk menemukan bilangan yang sama ketika dibutuhkan.

Dengan mengambil keunikan dari LCG yang membangkitkan bilangan yang sama dengan nilai inputan integer yang sama, pembangkit bilangan acak tersebut dapat digunakan untuk mengambil frame yang sama ketika di enkripsi dan didekripsi. Dengan menggunakan inputan integer yang diambil dari kunci AES, oleh karena itu dapat dilakukan penggabungan teknik steganografi dan kriptografi ke dalam media video PVD dengan menggunakan bantuan LCG dan AES untuk generate frame acak dan enkripsi pesan sebelum disisipkan ke dalam video.

3. METODE PENELITIAN

Pengumpulan data dilakukan dengan dua metode, yaitu dengan dokumentasi dari sumber, yaitu dari www.sample-videos.com, www.youtube.com, dan www.github.com dan mengambil studi pustaka dari berbagai media. Metode dokumentasuiyang digunakan untuk mendapatkan data penelitian dengan cara mengambil video dari situs internet, yaitu www.sample-videos.com, youtube.com, dan github.com. Secara global, metode yang diusulan di dalam penelitian ini adalah proses penyisipan pesan ke dalam video dan proses untuk pengambilan pesan dari dalam video yang sebelumnya sudah disisipkan pesan terlebih dahulu.

Pada proses penyisipan pesan, pesan rahasia di enkripsi terlebih dahulu dengan menggunakan algoritma AES agar pesan tersebut tidak diketahui oleh pihak ketiga. AES memerlukan sebuah input berupa kunci, kunci tersebut selain digunakan untuk proses enkripsi AES [12], juga akan digunakan untuk proses pengambilan frame dari dalam video cover yang sudah disiapkan dengan menggunakan algoritma LCG. Pada proses pengambilan pesan rahasia, alur yang dilakukan terbalik dengan proses penyisipan, yaitu dengan memasukkan kunci dari AES, yang akan mengekstraksi frame yang disisipkan pesan rahasia. Kemudian frame tersebut diambil pesan rahasia dengan menggunakan algoritma steganografi PVD, setelah didapatkan file pesan rahasia, file tersebut di dekripsi lagi dengan menggunakan algortima AES agar mendapat pesan rahasia yang dimaksud.

Hipotesis dari penjelasan di atas, pesan akan lebih aman disipkan jika sebelumnya sudah dienripsi terlebih dahulu dengan menggunakan AES, serta akan lebih sulit ketika akan diserang, karena frame yang disisipkan berdasarkan pembangkit bilangan acak LCG. Alur dari metode yang diusulkan seperti pada Gambar 1.

Sebelum menyisipkan pesan, cover video di pecah menjadi frame terlebih dahulu dan dipilih frame acak dengan menggunakan LCG melalui kunci enkripsi AES, kemudian teks rahasia dienkripsi dengan menggunakan AES, lalu frame yang dipilih menggunakan LCG akan digunakan sebagai media untuk penyisipan pesan dengan menggunakan algoritma steganografi PVD, terakhir frame-frame pecahan video tersebut digabung kembali menjadi video.

1. Langkah pertama dari proses penyisipan adalah mengkonversi dari video menjadi frame-frame yang nanti akan dipilih secara acak.
2. Frame tersebut kemudian diambil secara acak dengan menggunakan metode LCG. diasumsikan sudah mendapat angka dari kunci AES, dengan 3 angka dari kunci AES, akan bisa digunakan untuk membangkitkan bilangan acak dengan metode LCG. Contoh kunci AES menggunakan kunci AKU, dengan masing A, K, dan U mewakili a, b dan m, yaitu 65, 75, dan 85, dengan X = 0 sebagai awal.
3. Pesan yang akan disisipkan kemudian dienkripsi terlebih dahulu dengan menggunakan AES, dan terakhir disisipkan ke dalah frame yang sudah didapat tadi dengan menggunakan PVD.

4. HASIL DAN PEMBAHASAN

Video diistilahkan sebagai satu set frame yang diambil secara berurutan dengan waktu interval yang sangat kecil diantara mereka [4].Video mengacu pada informasi visual, termasuk gambar diam maupun bergerak. Istilah lain yang digunakan untuk menggantikan kata video adalah image sequence, karena gambar bergerak direpresentasikan dengan urutan banyak gambar diam dengan waktu tertentu. Video ditangkap oleh kamera yang dikompres dari scene tiga dimensi menjadi satu dimansi aliran data. Hanya dengan melihat sebuah scene dengan cahaya yang terlihat akan menguranginya ke proyeksi dua dimensi. Gambar yang bergerak dibuat oleh memindai scene yang sama secara berulang, yang membuat rangkaian titik-titik berwarna yang berulang. Mengkonversi warna dan intensitas dari setiap titik ke bentuk numerik akan memberikan representasi digital yang lengkap dari sebuah tampilan scene yang bergerak. Jenis video dibagi menjadi dua, yaitu video analog dan video digital.

Video digital adalah representasi dari visualisasi gambar yang bergerak yang dienkripsi sebagai data digital [7]. Video digital sangat kontras dengan video analog, yang merepresentasikan gambar yang bergerak dengan sinyal analog. Video digital terdiri dari serangkaian gambar yang ditampilkan secara berurutan. Sebaliknya, salah satu

metode analog, yaitu film motion picture, menggunakan serangkaian gambar yang diproyeksikan dengan cepat. Video digital dikenalkan pertama kali secara komersil pada tahun 1986 dengan format Sony D1, yang merekam standar komponen video terkompresi dalam bentuk digital. Sebagai tambahan untuk format yang tidak terkompresi, kompresi format video yang populer saat ini termasuk H.264 dan MPEG-4. Yang standar interkoneksi untuk video digital termasuk HDMI, Display Port, Digital Visual Interface (DVI), dan Serial Data Interface (SDI).

Dalam makalah ini, format file video yang digunakan untuk cover adalah avi yang didapatkan dari website gratis di engr.colostate.edu dengan durasi 3-6 detik dan kualitas video bebas. Pengujian kualitas video stego menggunakan MSE dan PSNR, waktu tempuh program, dan entropy untuk kriptografi. Langkah pertama dalam penyisipan pesan adalah dengan mengenkripsi terlebih dahulu plain teks. Contoh teks yang akan dienkripsi semisal "udinus", dan kunci "dian" proses pertama dalam enkripsi AES adalah merubah plaintext dan kunci menjadi bilangan hexadecimal. Langkah pertama dari proses penyisipan pesan adalah dengan mengubah pesan rahasia ke bentuk hexadecimal.

u d i n u s

Diubah ke bentuk decimal (ASCII) = 117 100 105 110 117 115
Lalu ubah dari bilangan decimal tersebut menjadi bilangan hexadecimal, sehingga menjadi sebagai berikut:

75 64 69 6E 75 73

Karena menggunakan AES, maka panjang plainteks dan kunci yang akan dienkripsi dan digunakan dirubah menjadi kelipatan 16. Lalu, langkah selanjutnya adalah merubah plainteks dan kunci menjadi hexadecimal. Pada Gambar 2, dapat dilihat proses penyisipan pesan secara runtut menggunakan AES-PVD pada video. Dilakukan percobaan dengan menginputkan pesan teks input langsung di dalam aplikasi matlab sesuai Gambar 1 dan Gambar 2.

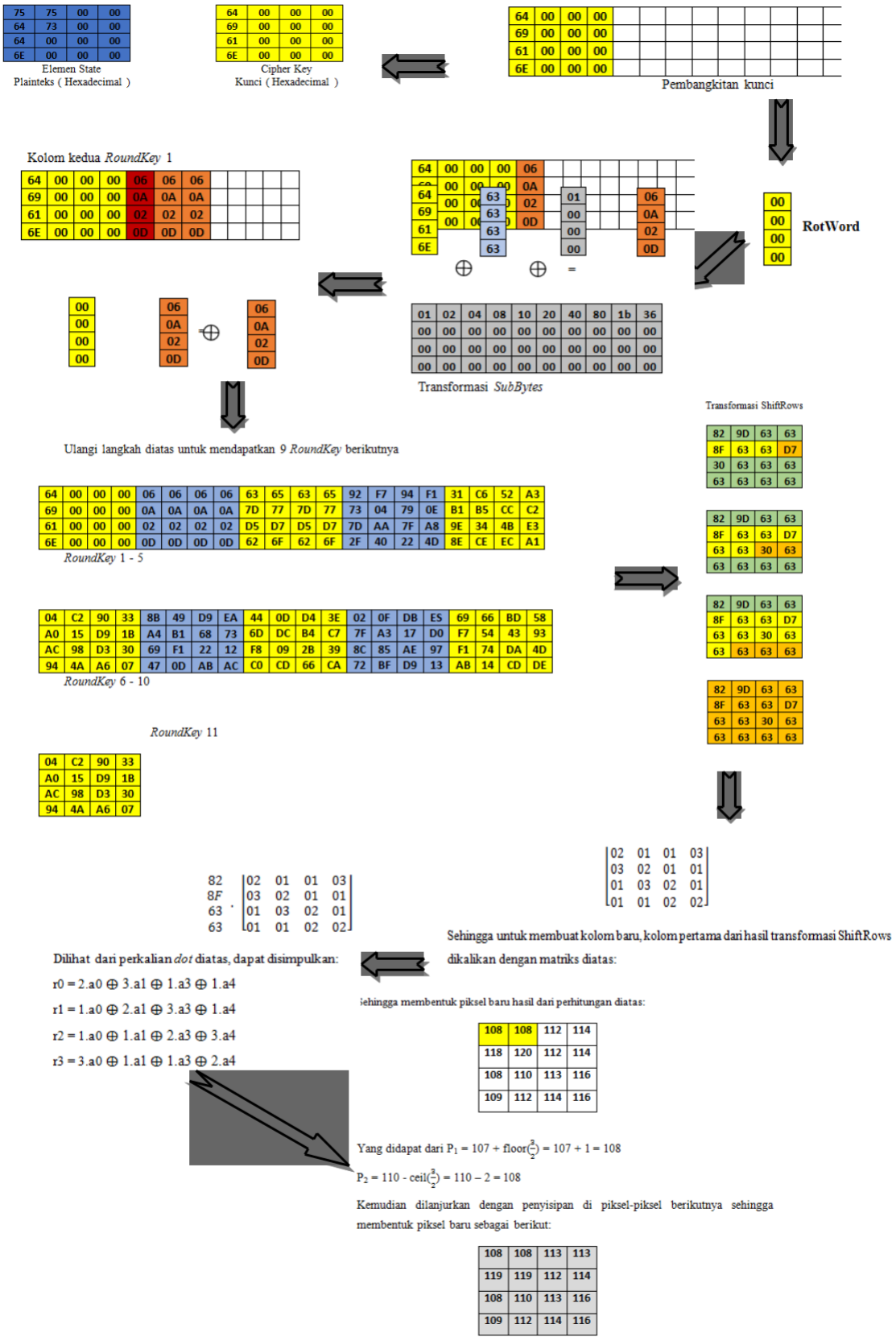
```
38
39      %mengambil pesan yang berada di message.txt
40      %  a = fopen('message.txt','r');
41      %  text = fread(a);
42      %  text = char(text)'
43      %menginputkan pesan yang akan dienkripsi
44 -    text = 'universitas dian nuswantoro'
45      %=========================================================================
46      %proses enkripsi dengan menggunakan AES
47
48 -    if length(kunci) > 16 % jika panjang kunci lebih dari 16
49 -        kunci = kunci(1:16); % ambil 16 digit pertama kunci
50 -    end
51 -    while mod(length(kunci),16) ~= 0 % selama panjang kunci bukan kelipatan 16
52 -        kunci = cat(2,kunci,char(0)); % tambahkan spasi
53 -    end
Command Window
```

Gambar 1. Input Kunci Teks.

Kemudian pesan input tersebut dienkripsi dengan menggunakan AES dan menggunakan kunci "dian".

```
kunci =

dian

>> cipher

cipher =

¾4□µZhÏ□vâ± mÊXGqÝ□□C -r□§□1    ¾

>>
```

Gambar 2. Enkripsi pesan.

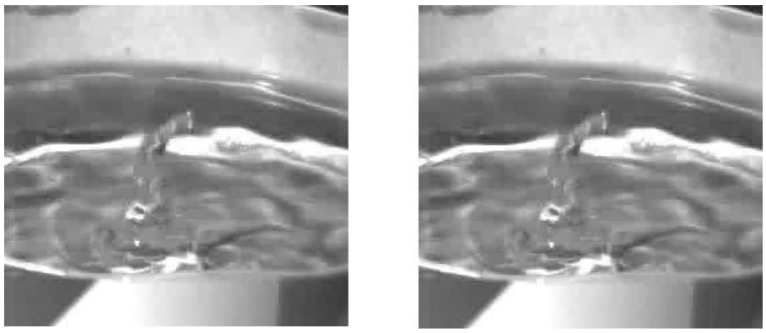


Gambar 3. Alur Kerja AES pada eksperimen ini.

Lalu setelah di enkripsi, langkah selanjutnya adalah mengubah video menjadi frame dengan algoritma sebagai berikut:

```
ii = 1; %untuk increment
while hasFrame(shuttleVideo) %jika masih mempunyai frame, iterasi masih berjalan
   img = readFrame(shuttleVideo); %membaca frame
   filename = [sprintf('%03d',ii) '.bmp']; %menyimpan nama file
   fullname = fullfile(workingDir,'out_frames2',filename); % mengambil semua nama file
dan directorynya
   imwrite(img,fullname) %menyimpan frame ke dalam directory yang sudah
   disiapkan ii = ii+1; %iterasi increment
end
```

Dengan inputan video bernama “drop.avi”, setelah dijalankan algoritma diatas, akan membentuk sebuah folder yang didalamnya terdapat frame-frame hasil dari video.



Frame asli Frame hasil se tgo

Gambar 4. Komparasi citra asli dan citra hasil stego.

Pada proses ekstraksi teks yang disembunyikan berhasil di dapat.

Gambar 5. Hasil dekripsi teks yang telah disispkan.

Didalam proses enkripsi dan dekripsi, program ditambah dengan elapsed time atau waktu yang dibutuhkan untuk proses enkripsi dan dekripsi, waktu berubah-ubah sesuai dengan kecepatan processor device dan banyaknya aplikasi yang sedang berjalan.

5. KESIMPULAN

Setelah disisipkan pesan ke dalam frame, frame hanya bisa dikonversi ke dalam video dalam bentuk uncompressed, karena jika di compress, nilai dari pesan yang disispkan tidak bisa dibaca. Nilai MSE rendah dan PSNR tinggi, itu berarti frame yang disisipkan tidak banyak berubah dan kualitas citra masih bagus. Pada percobaan dengan menyisipkan pesan dengan ukuran sebesar 21045 bit, MSE yang dihasilkan adalah 0.1096 dan PSNR sebesar 57.7341. Ada beberapa pengujian dengan video yang tidak disebutkan, tidak menemukan pesan rahasia meskipun video sudah di simpan dalam bentuk uncompressed. Di salah satu pengujian ada pesan yang dapat di retrieve dengan sempurna, yang berarti dalam frame yang disisipkan, di citra tersebut ada data lossy.

DAFTAR PUSTAKA

[1] C. A. Sari, E. H. Rachmawanto, D. W. Utomo, and R. R. Sani, "Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting," *Int. J. Appl. Intell. Syst.*, vol. 1, no. 3, pp. 179–190, 2016.

[2] E. H. Rachmawanto, R. S. Amin, D. R. I. M. Setiadi, and C. A. Sari, "A performance Analysis StegoCrypt Algorithm based on LSB-AES 128 bit in Various Image Size," in *International Seminar on Application for Technology of Information and Communication*, 2017, no. October 2017.

[3] S. N. Kishor, G. N. K. Ramaiah, and S. A. K. Jilani, "A review on steganography through multimedia," *Int. Conf. Res. Adv. Integr. Navig. Syst. RAINS 2016*, 2016.

[4] P. Yadav, N. Mishra, and S. Sharma, "A secure video steganography with encryption based on LSB technique," *2013 IEEE Int. Conf. Comput. Intell. Comput. Res. IEEE ICCIC 2013*, 2013.

[5] E. J. Kusuma, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, "An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption," in *International Conference on Innovative and Creative Information Technology (ICITech)*, 2017, pp. 1–5.

[6] H. K. Lee, J. C. Joo, and H. Y. Lee, "Improved steganographic method preserving pixel-value differencing histogram with modulus function," *EURASIP J. Adv. Signal Process.*, vol. 2010, 2010.

[7] R. J. Mstafa and K. M. Elleithy, "A highly secure video steganography using Hamming code (7, 4)," *2014 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2014*, 2014.

[8] O. Tornea, M. E. Borda, V. Pileczki, and R. Malutan, "DNA Vernam Cipher," *Proc. 3rd Int. Conf. E-Health Bioeng. - EHB 2011*, pp. 24–27, 2011.

[9] D. Nilesh and M. Nagle, "The new cryptography algorithm with high throughput," in *2014 International Conference on Computer Communication and Informatics*, 2014, pp. 1–5.

[10] M. Mohan, M. K. K. Devi, and V. J. Prakash, "Security Analysis and Modification of Classical Encryption Scheme," *Indian J. Sci. Technol.*, vol. 8, no. 8, pp. 542–548, 2015.

[11] R. Bhardwaj and V. Sharma, "Image Steganography Based on Complemented Message and Inverted Bit LSB Substitution," *Procedia Comput. Sci.*, vol. 93, no. September, pp. 832–838, 2016.

[12] N. Sharma, Prabhjot, and H. Kaur, "A Review of Information Security using Cryptography Technique.," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 4, pp. 323–326, 2017.