Available *online* at : http://bit.ly/InfoTekJar

InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan

ISSN (Print) 2540-7597 | ISSN (Online) 2540-7600

[1]Kriptografi

Pengamanan Citra Menggunakan Kombinasi Algoritma Kriptografi *Hill Cipher* dan Teknik Transposisi Segitiga

Windi Saputri Simamora, Syahril Efendi, Erna Budhiarti Nababan

Program Studi S2 Teknik Informatika, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Medan, Indonesia

KEYWORDS

Kriptografi, Citra, *Hill Cipher*, Transposisi Segitiga

CORRESPONDENCE

Phone: +628116131067

E-mail: syahril1@usu.ac.id

A B S T R A C T

Cara untuk mengamankan citra dapat dilakukan dengan kriptografi. Penelitian pada algoritma kriptografi sudah cukup banyak berkembang. Beberapa penelitian menyebutkan bahwa menggabungkan dua algoritma kriptografi dapat lebih meningkatkan keamanan dari citra dibandingkan dengan hanya satu algoritma. Penelitian ini melakukan enkripsi menggunakan kombinasi dua algoritma yaitu teknik transposisi segitiga dan *Hill Cipher*. Proses penggabungan dua algoritma dilakukan dengan terlebih dahulu mengenkripsi menggunakan teknik transposisi segitiga dan kemudian dilanjutkan dengan *Hill Cipher*. Begitu juga dengan proses dekripsi yang dilakukan secara kebalikannya. Pada penelitian ini menghasilkan performa yang lebih baik dibandingkan dengan menggunakan satu metode yang dapat dilihat pada nilai rata-rata MSE yang besar yaitu 10878,992 dan rata-rata PSNR yang kecil yaitu 0,781. Hal tersebut menandakan dengan menggabungkan dua algoritma dapat membuat pesan menjadi lebih aman. Metode dalam penelitian ini juga berhasil mengembalikan citra dangan baik tanpa adanya penambahan maupun pengurangan yang dapat dilihat dari hasil MSE dan PSNR yaitu 0 dan ∞.

PENDAHULUAN

Semakin meningkatnya perkembangan teknologi saat ini seperti komunikasi secara digital untuk bertukar pesan dari satu orang ke yang lainnya dalam aktivitas sehari-hari, sekolah maupun bekerja atau berbisnis [1]. Pesan yang digunakan dalam komunikasi yaitu berupa teks, dokumen, gambar maupun video [2]. Bentuk data digital yang sering dipakai adalah citra digital yang menyimpan data berupa foto atau gambar dalam bentuk digital. Saat data tersebut bersifat rahasia maka menyebabkan terdapatnya tantangan yaitu akses orang lain terhadap pesan sehingga pesan dapat dicuri orang lain dan disalahgunakan untuk hal negatif. Oleh karena itu diperlukan teknik untuk melindungi pesan tersebut yaitu kriptografi yang membuat gambar menjadi acak dan tidak dapat digunakan orang lain[3].

Kriptografi merupakan proses enkripsi dan dekripsi pesan untuk membuat pesan menjadi rahasia dengan mengubah pesan menjadi sulit dimengerti oleh orang lain [4], [5]. Salah satu algoritma kriptografi yang dapat digunakan adalah *Hill Cipher* yang merupakan algoritma kriptografi klasik yang menggunakan matrik dan aritmatika modulo sebagai kunci dalam prosesnya. *Hill Cipher* hanya memiliki satu kunci yaitu kunci privat atau rahasia[6]–[8].

Selain itu terdapat cara sederhana untuk mengenkripsi dan dekripsi pesan yaitu Teknik transposisi segitiga. Cara kerja teknik transposisi segitiga adalah dengan memasukkan karakter menjadi bentuk segitiga yang diawali satu karakter kemudian bertambah dua karakter menjadi tiga dan membentuk pola kelipatan ganjil lalu membacanya dari kolom segitiga yang paling kiri[9].

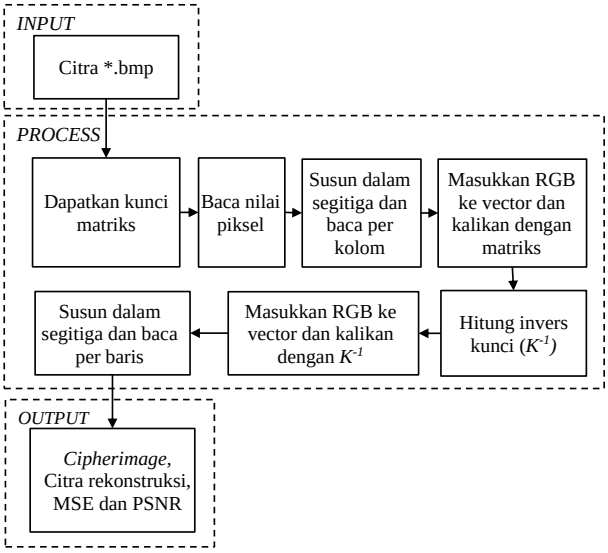
Algoritma *Hill Cipher* dan Teknik Transposisi Segitiga merupakan algoritma simetris yang memiliki kekurangan pada keamanan kuncinya yang menyebabkan orang lain dapat mengetahui pesan apabila diketahui kuncinya namun memiliki kelebihan waktu proses membutuhkan waktu yang singkat. Pada penelitian sebelumnya didapatkan hasil yaitu dengan menggabungkan dua algoritma kriptografi menghasilkan keamanan citra yang lebih baik dibandingkan hanya satu algoritma saja. Oleh karena itu pada penelitian ini dilakukan kombinasi menggunakan kedua algoritma yaitu *Hill Cipher* dan teknik transposisi segitiga agar menambah tingkat kesulitan pada pesan[10].

https://doi.org/10.30743/infotekjar.v6i2.4713

METODOLOGI PENELITIAN

Rancangan Penelitian

Metode untuk proses kriptografi yang digunakan dalam penelitian ini adalah Teknik transposisi segitiga dan *Hill Cipher* pada citra. Adapun rancangan dari penelitian dalam penggabungan kedua metode dapat dilihat pada diagram blok berikut berikut:



Tahapan dari proses enkripsi dan dekripsi dilakukan secara berurutan. Tahap awal dimulai dengan mengenkripsi citra menggunakan Teknik transposisi segitiga, setelah itu dilanjutkan dengan proses enkripsi menggunakan *Hill Cipher* dengan terlebih dahulu membangkitkan kunci matriks secara acak sesuai dengan ketentuan kunci *Hill Cipher*. Proses dekripsi merupakan kebalikan dari proses enkripsi yaitu dengan melakukan dekripsi *Hill Cipher* terlebih dahulu lalu dilanjutkan dengan dekripsi menggunakan Teknik transposisi segitiga [11]. Kombinasi pada proses enkripsi diharapkan dapat mempersulit pesan untuk dipecahkan.

Proses Enkripsi Citra Digital

Kombinasi proses enkripsi dimulai dengan mengambil nilai piksel dari citra kemudian dienkripsi terlebih dahulu menggunakan teknik transposisi segitiga kemudian dienkripsi lagi dengan *Hill Cipher* sehingga menghasilkan *cipherimage* yang sudah teracak.

Contoh diberikan sebagian piksel berukuran 3 × 3 seperti berikut ini:

(237,101,198)	(151,151,151)	(39,77,52)
(68,197,17)	(39,77,52)	(131,15,98)
(42,37,79)	(122,171,230)	(249,180,43)

Gambar 1. Piksel citra berukuran 3 × 3

Tahapan enkripsi dapat dilakukan dengan tahap berikut:

1. Transposisikan citra ke dalam segitiga

		237,101,198		
	151,151,151	39,77,52	68,197,17	
39,77,52	131,15,98	42,37,79	122,171,230	249,180,43

2. Baca nilai dari kolom paling kiri

(39,77,52) (151,151,151) (131,15,98)
(237,101,198) (39,77,52) (42,37,79)
(68,197,17) (122,171,230) (249,180,43)

3. Lakukan enkripsi dengan *Hill Cipher*

Diberikan kunci matriks yang *invertible* berikut:

$$K = \begin{bmatrix} 1 & 2 & 11 \\ 5 & 4 & 10 \\ 7 & 3 & 9 \end{bmatrix}$$

Susun nilai RGB setiap piksel citra menjadi vector yang dapat dikalikan sesuai ukuran kunci matriks kemudian kalikan dengan kunci matriks seperti berikut:

❖ $\begin{bmatrix} 39 & 77 & 52 \\ 151 & 151 & 151 \\ 131 & 15 & 98 \end{bmatrix} \times \begin{bmatrix} 1 & 2 & 11 \\ 5 & 4 & 10 \\ 7 & 3 & 9 \end{bmatrix} =$

$\begin{bmatrix} 788 & 542 & 167 \\ 1963 & 1359 & 4530 \\ 892 & 616 & 2473 \end{bmatrix} (mod\ 256) = \begin{bmatrix} 20 & 30 & 131 \\ 171 & 79 & 178 \\ 124 & 104 & 169 \end{bmatrix}$

❖ $\begin{bmatrix} 237 & 101 & 198 \\ 39 & 77 & 52 \\ 42 & 37 & 79 \end{bmatrix} \times \begin{bmatrix} 1 & 2 & 11 \\ 5 & 4 & 10 \\ 7 & 3 & 9 \end{bmatrix} =$

$\begin{bmatrix} 2128 & 1471 & 5399 \\ 788 & 542 & 1667 \\ 780 & 469 & 1543 \end{bmatrix} (mod\ 256) = \begin{bmatrix} 80 & 192 & 23 \\ 20 & 30 & 131 \\ 12 & 213 & 7 \end{bmatrix}$

❖ $\begin{bmatrix} 69 & 197 & 17 \\ 122 & 171 & 230 \\ 249 & 180 & 43 \end{bmatrix} \times \begin{bmatrix} 1 & 2 & 11 \\ 5 & 4 & 10 \\ 7 & 3 & 9 \end{bmatrix} =$

$\begin{bmatrix} 1173 & 977 & 2822 \\ 2587 & 1618 & 5122 \\ 1450 & 1347 & 4926 \end{bmatrix} (mod\ 256) = \begin{bmatrix} 149 & 209 & 66 \\ 27 & 82 & 2 \\ 170 & 67 & 62 \end{bmatrix}$

4. Susun hasil perkalian matriks ke dalam nilai piksel citra dan didapatkan *cipherimage* berikut:

(20,30,131)	(171,79,178)	(124,104,247)
(80,192,23)	(20,30,131)	(12,213,7)
(149,209,66)	(27,82,2)	(170,67,62)

Gambar 2. *Cipherimage* citra berukuran 3 × 3 piksel

Proses Dekripsi Citra Digital

Untuk mengembalikan citra menjadi citra yang asli dilakukan proses dekripsi. Tahap dekripsi merupakan kebalikan dari proses enkripsi, jika tahap pertama dalam enkripsi menggunakan Teknik transposisi segitiga maka tahap pertama dalam proses dekripsi menggunakan *Hill Cipher* [12]. Tahap untuk mendekripsi *cipherimage* pada gambar 2 dapat dilakukan dengan mengalikan nilai RGB setiap pixel dengan nilai invers dari kunci matriks sebagai berikut:

1. Dekripsi menggunakan *Hill Cipher*

Invers matriks dari kunci $K = \begin{bmatrix} 1 & 2 & 11 \\ 5 & 4 & 10 \\ 7 & 3 & 9 \end{bmatrix}$ adalah $K^{-1} = \begin{bmatrix} 150 & 247 & 168 \\ 241 & 92 & 229 \\ 59 & 147 & 106 \end{bmatrix}$ maka, K^{-1} digunakan untuk proses dekripsi.

❖ $\begin{bmatrix} 20 & 30 & 131 \\ 171 & 79 & 178 \\ 124 & 104 & 169 \end{bmatrix} \times \begin{bmatrix} 150 & 247 & 168 \\ 241 & 92 & 229 \\ 59 & 147 & 106 \end{bmatrix} =$

$\begin{bmatrix} 17959 & 26957 & 24116 \\ 55191 & 75671 & 65687 \\ 53635 & 65039 & 62562 \end{bmatrix} (mod\ 256) = \begin{bmatrix} 39 & 77 & 52 \\ 151 & 151 & 151 \\ 131 & 15 & 98 \end{bmatrix}$

❖ $\begin{bmatrix} 80 & 192 & 23 \\ 20 & 30 & 131 \\ 12 & 213 & 7 \end{bmatrix} \times \begin{bmatrix} 150 & 247 & 168 \\ 241 & 92 & 229 \\ 59 & 147 & 106 \end{bmatrix} =$

$\begin{bmatrix} 59629 & 40805 & 59846 \\ 17959 & 26957 & 24116 \\ 53546 & 23589 & 51535 \end{bmatrix} (mod\ 256) = \begin{bmatrix} 237 & 101 & 198 \\ 39 & 77 & 52 \\ 42 & 37 & 79 \end{bmatrix}$

https://doi.org/10.30743/infotekjar.v6i2.4713

❖ $\begin{bmatrix}149 & 209 & 66\\ 27 & 82 & 2\\ 170 & 67 & 62\end{bmatrix} \times \begin{bmatrix}150 & 247 & 168\\ 241 & 92 & 229\\ 59 & 147 & 106\end{bmatrix} = \begin{bmatrix}76613 & 65733 & 79889\\ 23930 & 14507 & 23526\\ 45305 & 57268 & 50475\end{bmatrix} (mod\ 256) = \begin{bmatrix}69 & 197 & 17\\ 122 & 171 & 230\\ 249 & 180 & 43\end{bmatrix}$

2. Transposisikan ke dalam segitiga dari kolom paling kiri.

		237,101,198		
	151,151,151	39,77,52	68,197,17	
39,77,52	131,15,98	42,37,79	122,171,230	249,180,43

3. Baca nilai RGB dari baris pertama sehingga didapatkan nilai piksel citra seperti citra asli berikut:

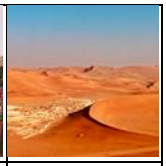
(237,101,198)	(151,151,151)	(39,77,52)
(68,197,17)	(39,77,52)	(131,15,98)
(42,37,79)	(122,171,230)	(249,180,43)

Gambar 3. Piksel citra rekonstruksi

HASIL DAN PEMBAHASAN

Pada penelitian ini data yang diuji dalam penelitian ini adalah citra digital yang berformat *.bmp dengan ukuran berbeda-beda. Nilai RGB dari setiap piksel akan diambil dan proses menggunakan system modulo 256 karena setiap komponen piksel memiliki Panjang bit 8 (0-255). Kunci matriks yang digunakan adalah matriks berukuran 3 × 3 yang *invertible*. Citra yang akan diuji dapat dilihat pada tabel sebagai berikut[13]:

Tabel 1. Data Citra Digital

			
250 × 250 *piksel*	350 × 350 *piksel*	450 × 450 *piksel*	500 × 500 *piksel*
			
600 × 600 *piksel*	700 × 700 *piksel*	800 × 800 *piksel*	900 × 900 *piksel*
			
950 × 950 *piksel*	1000 × 1000 *piksel*		

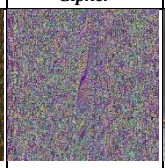
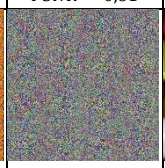
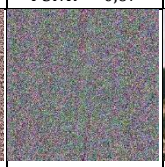
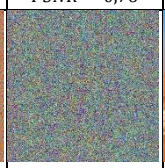
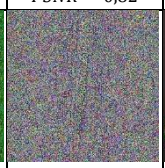
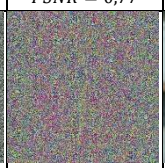
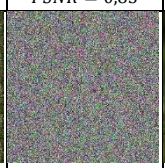
Pengujian tingkat keamanan citra dilihat dengan membandingkan citra asli dengan cipherimage dengan menghitung nilai *Mean Squared Error (MSE)* dan *Peak Signal to Noise Ratio (PSNR)*. Selain itu nilai MSE dan PSNR juga digunakan untuk melihat keutuhan data dari citra yang telah dikembalikan seperti semula. Nilai tersebut digunakan untuk melihat kualitas citra dari *cipherimage* maupun citra rekonstruksi. Rumus untuk menghitung MSE dan PSNR dapat dilihat seperti berikut.

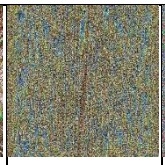
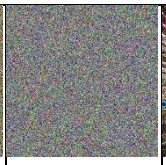
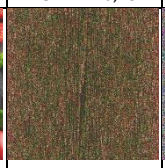
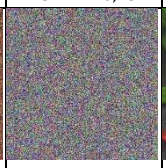
$$MSE = \frac{1}{N \cdot M} \sum_{i=1}^{M} \sum_{j=1}^{N} (f(i,j) - f'(i,j))^2 \quad (1)$$

$$PNSR = 10 \log \frac{s^2}{MSE} \quad (2)$$

Dimana *M* adalah panjang citra (dalam pixel), *N* adalah lebar citra (dalam pixel), $f(i,j)$ adalah intensitas citra di titik (i,j) citra asli, $f'(i,j)$ adalah intensitas citra di titik (i,j) citra hasil dan s merupakan nilai maksimum dari pixel citra yang digunakan misalnya s=255 untuk gambar 8-bit [14]. Hasil pengujian enkripsi dan dekripsi dapat dilihat pada tabel 2.

Tabel 2. Citra Hasil Proses Enkripsi dan Dekripsi

Citra Asli	Enkripsi Transposisi Segitiga	Enkripsi Transposisi Segitiga + *Hill Cipher*	Dekripsi
			
250 × 250 *piksel*	$MSE = 3871{,}6$ $PSNR = 1{,}23$	$MSE = 10018{,}54$ $PSNR = 0{,}81$	$MSE = 0$ $PSNR = \infty$
			
350 × 350 *piksel*	$MSE = 8464{,}27$ $PSNR = 0{,}89$	$MSE = 13999{,}45$ $PSNR = 0{,}67$	$MSE = 0$ $PSNR = \infty$
			
450 × 450 *piksel*	$MSE = 12328{,}27$ $PSNR = 0{,}72$	$MSE = 11319{,}08$ $PSNR = 0{,}76$	$MSE = 0$ $PSNR = \infty$
			
500 × 500 *piksel*	$MSE = 5982{,}85$ $PSNR = 1{,}04$	$MSE = 9907{,}39$ $PSNR = 0{,}82$	$MSE = 0$ $PSNR = \infty$
			
600 × 600 *piksel*	$MSE = 6434{,}47$ $PSNR = 1$	$MSE = 11169{,}2$ $PSNR = 0{,}77$	$MSE = 0$ $PSNR = \infty$
			
700 × 700 *piksel*	$MSE = 6741{,}89$ $PSNR = 0{,}98$	$MSE = 9138{,}25$ $PSNR = 0{,}85$	$MSE = 0$ $PSNR = \infty$
			
800 × 800 *piksel*	$MSE = 6386{,}24$ $PSNR = 1{,}01$	$MSE = 11651{,}24$ $PSNR = 0{,}75$	$MSE = 0$ $PSNR = \infty$

			
900 × 900 *piksel*	$MSE = 8409{,}79$ $PSNR = 0{,}89$	$MSE = 9802{,}59$ $PSNR = 0{,}82$	$MSE = 0$ $PSNR = \infty$
Citra Asli	**Enkripsi Transposisi Segitiga**	**Enkripsi Transposisi Segitiga + *Hill Cipher***	**Dekripsi**
			
950 × 950 *piksel*	$MSE = 11518{,}26$ $PSNR = 0{,}75$	$MSE = 12117{,}85$ $PSNR = 0{,}73$	$MSE = 0$ $PSNR = \infty$
			
1000 × 1000 *piksel*	$MSE = 3730{,}76$ $PSNR = 1{,}24$	$MSE = 9666{,}33$ $PSNR = 0{,}83$	$MSE = 0$ $PSNR = \infty$

Tabel 2 menunjukkan bahwa hasil perhitungan MSE pada enkripsi menggunakan transposisi segitiga didapatkan hasil yang lebih kecil daripada enkripsi menggunakan metode yang ditawarkan. Hal tersebut menandakan metode dalam penelitian ini lebih mempersilit citra utuk dikenali karena hasil *cipherimage* menjadi lebih acak. Begitu jugan dengan hasil PSNR pada enkripsi menggunakan metode yang diusulkan dihasilkan nilai yang lebih kecil dibandingkan dengan menggunakan transposisi segitiga saja. Semakin kecil nilai PSNR yang dihasilkan menandakan tingkat kemiripan citra yang lebih jauh dan kualitas yang lebih buruk.

Pengujian kualitas citra yang telah dikembalikan setelah proses dekripsi didapatkan nilai $MSE = 0$ dan $PSNR = \infty$ yang menandakan kualitas citra rekonstruksi memiliki kemiripan dengan citra asli dan tidak adanya penyisipan, penambahan maupun pengurangan pada citra.

Hasil pengujian dari metode yang diusulkan yaitu Teknik transposisi segitiga dan *Hill Cipher* dapat dilihat pada tabel 3.

Tabel 3. Hasil MSE dan PSNR Proses Enkripsi dan Dekripsi

Citra Asli	Enkripsi		Dekripsi	
	MSE	PSNR	MSE	PSNR
250 × 250 *piksel*	10018,54	0,81	0	∞
350 × 350 *piksel*	13999,45	0,67	0	∞
450 × 450 *piksel*	11319,08	0,76	0	∞
500 × 500 *piksel*	9907,39	0,82	0	∞
600 × 600 *piksel*	11169,2	0,77	0	∞
700 × 700 *piksel*	9138,25	0,85	0	∞
800 × 800 *piksel*	11651,24	0,75	0	∞
900 × 900 *piksel*	9802,59	0,82	0	∞
950 × 950 *piksel*	12117,85	0,73	0	∞
1000 × 1000 *piksel*	9666,33	0,83	0	∞
Rata-rata	10878,992	0,781	0	∞

Dari tabel 3 diatas dapat dilihat bahwa metode enkripsi menggunakan gabungan transposisi segitiga dan *Hill Cipher* menghasilkan performa yang baik dan dapat mengembalikan citra dengan baik.

KESIMPULAN

Berdasarkan hasil akhir dari pengujian yang diperoleh pada pembahasan di atas maka beberapa hal yang dapat disimpulkan adalah pada penelitian ini melakukan enkripsi menggunakan gabungan teknik trasposisi segitiga dan *Hill Cipher* menghasilkan performa yang lebih baik dibandingkan hanya menggunakan satu metode saja yang dapat dilihat pada hasil penelitian di atas. Hasil tersebut dibuktikan dengan nilai rata-rata MSE yang besar yaitu 10878,992 dan rata-rata PSNR yang kecil yaitu 0,781. Hal tersebut menandakan dengan menggabungkan dua algoritma dapat membuat pesan menjadi lebih aman. Metode dalam penelitian ini juga berhasil mengembalikan citra dangan baik tanpa adanya penambahan maupun pengurangan yang dapat dilihat dari hasil MSE dan PSNR yaitu 0 dan ∞.

REFERENSI

[1] D. Rachmawati, M. A. Budiman, and C. A. Saffiera, 'An Implementation Of Elias Delta Code And ElGamal Algorithm In Image Compression And Security', *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 300, p. 012040, Jan. 2018, doi: 10.1088/1757-899X/300/1/012040.

[2] H. Touil, N. E. Akkad, and K. Satori, 'Text Encryption: Hybrid cryptographic method using Vigenere and Hill Ciphers.', in *2020 International Conference on Intelligent Systems and Computer Vision (ISCV)*, Fez, Morocco, Jun. 2020, pp. 1–6. doi: 10.1109/ISCV49265.2020.9204095.

[3] Supiyanto and S. A. Mandowen, 'Advanced hill cipher algorithm for security image data with the involutory key matrix', *J. Phys. Conf. Ser.*, vol. 1899, no. 1, p. 012116, May 2021, doi: 10.1088/1742-6596/1899/1/012116.

[4] D. Rachmawati, M. A. Budiman, and L. Aulya, 'Three-pass protocol scheme for bitmap image security by using vernam cipher algorithm', *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 308, p. 012003, Feb. 2018, doi: 10.1088/1757-899X/308/1/012003.

[5] Handrizal, Herriyance, J. Hanayong, M. Zarlis, and P. Sihombing, 'Implementation of Image Security using Elliptic Curve Cryptography RSA Algorithm and Least Significant Bit Algorithm', *J. Phys. Conf. Ser.*, vol. 1898, no. 1, p. 012016, Jun. 2021, doi: 10.1088/1742-6596/1898/1/012016.

[6] D. Rachmawati, M. A. Budiman, and M. I. Wardhono, 'Hybrid Cryptosystem for Image Security by Using Hill Cipher 4x4 and ElGamal Elliptic Curve Algorithm', in *2018 IEEE International Conference on Communication, Networks and Satellite (Comnetsat)*, Medan, Indonesia, Nov. 2018, pp. 49–54. doi: 10.1109/COMNETSAT.2018.8684121.

[7] M. Lakhera, M. M. S. Rauthan, and A. Agarwal, 'Securing biometric template using double hill cipher with self-invertible key and random permutation of pixels locations', in *2016 2nd International Conference on Next Generation Computing Technologies (NGCT)*, Dehradun, India, Oct. 2016, pp. 814–817. doi: 10.1109/NGCT.2016.7877522.

https://doi.org/10.30743/infotekjar.v6i2.4713

[8] J. R. Paragas, A. M. Sison, and R. P. Medina, 'Hill Cipher Modification: A Simplified Approach', in *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, Chongqing, China, Jun. 2019, pp. 821–825. doi: 10.1109/ICCSN.2019.8905360.

[9] M. A. Budiman and A. Sharif, 'Implementasi Operasi XOR dan Teknik Transposisi Segitiga untukPengamanan Citra JPEG Berbasis Android', p. 17.

[10] V. M. Putrie, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, 'Super Encryption using Transposition-Hill Cipher for Digital Color Image', in *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, Yogyakarta, Indonesia, Nov. 2018, pp. 152–157. doi: 10.1109/ISRITI.2018.8864361.

[11] A. A. M. Khalaf, M. S. Abd El-Karim, and H. F. A. Hamed, 'Proposed triple hill cipher algorithm for increasing the security level of encrypted binary data and its implementation using FPGA', in *2015 17th International Conference on Advanced Communication Technology (ICACT)*, Seoul, Jul. 2015, pp. 454–459. doi: 10.1109/ICACT.2015.7224836.

[12] A. Agung, N. Heryana, and A. Solehudin, 'Combination of Hill Cipher Algorithm and Caesar Cipher Algorithm for Exam Data Security', *Buana Inf. Technol. Comput. Sci. BIT CS*, vol. 1, no. 2, pp. 42–45, Jul. 2020, doi: 10.36805/bit-cs.v1i2.1072.

[13] Unsplash, 'Visual search | Unsplash'. https://unsplash.com/s/visual/c51985ce-208a-44c5-9666-f79dd84acfd2 (accessed Nov. 30, 2021).

[14] V. Praveena, P. H. Manohara Varma, and B. Raju, 'Image Encryption using SCAN Patterns & Hill Cipher', in *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, India, May 2018, pp. 1983–1988. doi: 10.1109/RTEICT42901.2018.9012499.