ISBN: 9-789-7936-499-93

IMPLEMENTASI ONE TIME PAD KRIPTOGRAFI PADA GAMBAR GRAYSCALE DAN GAMBAR BERWARNA

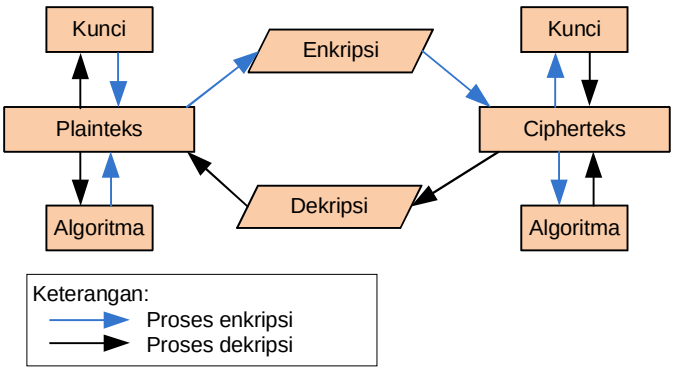
De Rosal Ign. Moses Setiadi[1], Eko Hari Rachmawanto[2], Christy Atika Sari[3]
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
Jl. Imam Bonjol 207 Semarang, 50131
Telp. (024) 3517261
E-mail: moses@dsn.dinus.ac.id[1], eko.hari@dsn.dinus.ac.id[2], atika.sari@dsn.dinus.ac.id[3]

ABSTRAK
Penyandian pesan melalui teknik kriptografi terus berkembang, salah satunya yaitu penggunaan algoritma One Time Pad (OTP) yang semula hanya digunakan untuk menyandikan tulisan kini dapat digunakan untuk menyandikan gambar. OTP merupakan algoritma kriptografi klasik kunci simetris yang sangat aman untuk menyandikan gambar, bahkan sampai saat ini beklum terpecahkan. Hal ini dikarenakan panjang kunci yang digunakan sama dengan panjang plainteks yang dalam pengoperasiannya harus dalam keadaan random dan tidak boleh digenerate. Hasil eksperimen diuji menggunaan Peak Signal to Noise Ratio (PSNR), Bit Error Ratio (BER), Cross Correlation (CC). Pada kriptografi, nilai PSNR semakin mendekati 0 artinya gambar tersandikan sempurna yang bertolak belakang dengan watermarking. Pada watermarking nilai PSNR lebih dari 40 dB membuktikan tingkat keberhasilan yang baik. Makalah ini menyajikan hasil eksperimen pada 24 gambar keabuan dan gambar berwarna untuk proses enkripsi dan dekripsi. Hasil PSNR proses enkripsi terbaik yaitu 7,4134 dB, BER 26230 sedangkan proses dekripsi berhasil dengan bukti nilai PSNR infinitive, BER dan MSE dari seluruh gambar bernilai 0. Untuk mengetahui perbedaan gambar asli dengan gambar hasil kriptografi, perbedaan nilai dari hasil percobaan disajikan dalam bentuk histogram.

Kata Kunci: One Time Pad, Kriptografi, Citra, PSNR, BER

6. PENDAHULUAN

Beberapa teknik penyembunyian data seperti kriptografi dan steganografi terus dikembangkan dengan tujuan untuk mengamankan data. Kriptografi merupakan ilmu untuk mengamankan data dalam operasi penyandian pada algoritma tertentu (Munir 2011), dimana teknik ini sudah ada sejak zaman romawi kuno. Semula kriptografi digunakan untuk menyandikan informasi mengenai peperangan pada perang dunia II, namun kini kriptografi telah dikembangkan sampai peyandian dengan media berupa IP address. Media yang paling populer pada kriptografi yaitu teks dan gambar. Proses penyandian dan ekstraksi pada kriptografi dapat dilihat pada Gambar 1.



Gambar 1. Alur Kerja Teknik Kriptografi

Seperti terlihat pada Gambar 1, dalam kriptografi terdapat proses penyandian data dan dekripsi data. Porses penyandian data yaitu menyandikan plainteks ke dalam bentuk lain yang tidak terdeteksi. Model data yang tidak terdeteksi ini disebut proses dekripsi data. Plainteks merupakan data asli atau data induk dapat berupa teks, gambar, audio, video maupun IP address. Bentuk cipherteks biasanya mengikuti format asli dari plainteksnya. Operasi kriptografi umunya menggunakan algoritma tertentu misalnya pada kriptografi klasik kunci simteris yang digunakan dalam makalah ini yaitu One Time Pad (OTP).

ISBN: 9-789-7936-499-93

7. STATE OF THE ART

Beberapa penelitian mengenai kriptografi dengan algoritma One Time Pad (OTP) telah dilakukan menggunakan media yang berbeda seperti pada Tabel 1.

Tabel 1. *State of The Art*

Tahun	*Author dan Tahun Penelitian*	*Algoritma*	*Jenis Citra*
2010	Jeyamala.C, GopiGanesh.S, & G.S(Jeyamala et al. 2010)	OTP + Chaos Functions	Citra grayscale
2014	Sari, CA, Rachmawanto, EH (Sari & Rachmawanto 2014)	Vernam Cipher + End of File	File Pdf
2014	Liansheng, Wengang, Kuaikuai, & Zhiqiang(Liansheng et al. 2014)	Logistic Map	Citra grayscale
2015	Li, Xing, Qu, & Zhang(Li et al. 2015)	Tent +Lorenz Chaotic Systems	Citra grayscale
2015	Rachmawanto, EH, Sari, CA (Rachmawanto & Sari 2015)	Shift Cipher	File Doc
2016	Sekertekin (Sekertekin & Atan 2016)	Ikeda + Henon Maps	Citra RGB
2016	Jain & Sharma(Jain & Lenka 2015)	Fractional DRPM + Chaotic Baker Map	Citra RGB
2016	Astuti, YP, dkk (Astuti et al. 2016)	Blowfish	Teks
2016	Sari, CA, dkk (Sari & Rachmawanto 2016)	Vernam Cipher + Bit Shiffting	Semua jenis file
2017	M Setiadi, De Rosal Ign, dkk (Ignatius et al. 2017)	One Time Pad	Citra Grayscale
2017	Erawan, L, dkk (Erawan, et al. 2017)	One Time Pad	Semua jenis file

Pada penelitian yang dilakukan oleh ADDIN CSL_CITATION { "citationItems" : [{ "id" : "ITEM-1", "itemData" : { "author" : [{ "dropping-particle" : "", "family" : "Ignatius", "given" : "De Rosal", "non-dropping-particle" : "", "parse-names" : false, "suffix" : "" }, { "dropping-particle" : "", "family" : "Setiadi", "given" : "Moses", "non-dropping-particle" : "", "parse-names" : false, "suffix" : "" }, { "dropping-particle" : "", "family" : "Rachmawanto", "given" : "Eko Hari", "non-dropping-particle" : "", "parse-names" : false, "suffix" : "" }], "container-title" : "Journal of Applied Intelligent System", "id" : "ITEM-1", "issue" : "1", "issued" : { "date-parts" : [["2017"]] }, "page" : "1-11", "title" : "Secure Image Steganography Algorithm Based on DCT with OTP Encryption", "type" : "article-journal", "volume" : "2" }, "uris" : ["http://www.mendeley.com/documents/?uuid=f12c344d-e62d-48d0-a035-815dd0c1c856"] }], "mendeley" : { "formattedCitation" : "(Ignatius et al. 2017)", "plainTextFormattedCitation" : "(Ignatius et al. 2017)", "previouslyFormattedCitation" : "(11)" }, "properties" : { "noteIndex" : 0 }, "schema" : "https://github.com/citation-style-language/schema/raw/master/csl-citation.json" }(Ignatius et al. 2017) (Erawan etl al. 2017) mengatakan hal yang sama tentang OTP, dimana OTP sangat susah dipecahkan yang terbukti secara matematis. Penelitian kriptografi pada citra juga telah banyak dilakukan, salah satunya adalah pada penelitian (Jeyamala et al. 2010) menggunakan metode one time pad dan chaos approach yang diterapkan pada citra grayscale dimana hasil percobaan menunjukkan bahwa algoritma tersebut secara signifikan menolak terhadap serangan statistik. Selain itu, dengan prinsip kerja algoritma tersebut secara signifikan kuat terhadap serangan *brute force* dan tes sensitivitas kunci. Waktu yang dibutuhkan untuk enkripsi relatif cukup cepat dibandingkan dengan algoritma lain. Sehingga membuat kombinasi algoritma cocok untuk enkripsi gambar dalam aplikasi real time.

8. METODE PENELITIAN

1.1. Kriptografi Simetris dan Asimetris

Jenis kriptografi berdasarkan kemunculannya yaitu klasik dan modern. Kriptografi klasik biasanya menggunakan media berupa teks, namun pada makalah ini akan digunakan media gambar. Baik kriptografi klasik dan kriptografi modern, keduanya dapat dioperasikan dalam dua jenis kunci yaitu simetris dan asimetris. Kriptografi klasik simetris

ISBN: 9-789-7936-499-93

dengan model operasi stream cipher yaitu misalnya RC4, blowfish, vigenere cipher, beaufort, autokey, sedangkan pada model operasi blok cipher yaitu One Time Pad (OTP) (Sari et al. 2016). Kriptografi klasik dengan model operasi blok cipher umumnya menggunakan perhitungan XOR. Teknik data hiding yang baik harus memenuhi aspek imperceptibility (ketidaknampakan oleh mata manusia), aspek robustness (tahan terhadap serangan), dan aspek payload. Pada kenyataannya tidak semua hasil operasi pada data hiding dapat memenuhi seluruh aspek tersebut.

1.2. One Time Pad (OTP)

One Time Pad merupakan salah satu algoritma yang populer dan sering digunakan dalam teknik kriptografi. OTP termasuk kelompok algoritma yang simetris dalam kriptografi dimana kunci enkripsi dan dekripsi dalam bentuk dan panjang yang sama, serta menggunakan operasi XOR(Ignatius et al. 2017). Keunggulan OTP adalah sangat sulit untuk dipecahkan tapi memiliki kekurangan dimana kunci yang digunakan kadang terlalu panjang karena harus menyesuaikan jumlah karakter yang akan dienkripsi(Tornea et al. 2011).Dari semua metode kriptografi yang telah dirancang, OTP adalah metode yang telah terbukti benar-benar aman secara matematis.One Time Pad bisa dikatakan 'sempurna' jika memenuhi kondisi berikut (Sari et al. 2016)kunci harus sepanjang plainteks, kunci harus acak seluruhnya atau sepenuhnya berbeda, kunci hanya sekali digunakan setiap melakukan enkripsi, danhanya terdapat dua salinan dari kunci: satu untuk pengirim dan satu untuk penerima(Shukla et al. 2013). Rumus enkripsi dan dekripsi OTP dalam dijabarkan melalui Persamaan 1 dan Persamaan 2.

$$Cc = (Ca + k) \bmod X \quad (1)$$

dimana:
Cc = Citra cipher,
Ca = Citra asli,
k = kunci random.
X = nilai maksimal intensitas citra

Sedangkan untuk melakukan dekripsi menggunakan rumus:

$$Ca = (Cc - k) \bmod X \quad (2)$$

1.3. Pengukuran Kualitas Citra

Pada makalah ini akan digunakan tiga buah cara yaitu Peak Signal to Noise Ratio (PSNR) (Ignatius et al. 2017) dan BER (Bit Error Ratio) serta untuk membuktikan bahwa gambar terlah dienkripsi atau didekripsi dapat dilihat menggunakan histogram gambar. PSNR merupakan perhitungan untuk mengetahui perbandingan dari nilai maksimal sinyal suatu gambar sehingga akan diketahui nilai gambar sebelum dan sesudah disiipi oleh gambar pesan seperti terlihat pada Persamaan 3 dan Persamaan 4 berikut.

$$MSE = \frac{1}{MN}\sum_{X=1}^{M}\sum_{y=1}^{N}(a_{xy} - b_{xy})^2 \quad (3)$$

$$PSNR = 10\,Log_{10}\left(\frac{a^2max}{MSE}\right) \quad (4)$$

Dimana:
x, y = koordinat gambar
M,N = dimensi gambar
a = gambar hasil enkripsi
b = gambar asli (sebelum enkripsi)

Sedangkan BER merupakan perkiraan probabilitas kesalahan bit pada suatu gambar atau dapat diartikan sebagai jumlah bit salah dalam suatu gambar, dimana cara perhitungan yang digunakan yaitu mengurangkan jumlah bit salah pada gambar hasil operasi dengan jumlah bit pada gambar asli.

9. HASIL EKSPERIMEN

Pada makalah ini gambar yang digunakan untuk penelitian berupa gambar berwarna dan gambar grayscale sejumlah 20 gambar berformat bmp. Contoh beberapa gambar yang digunakan tampak pada Gambar 2.

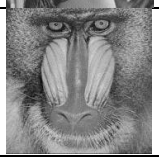
ISBN: 9-789-7936-499-93

Baboon.bmp Cameraman.bmp Lena.bmp Peppers.bmp

Gambar 2. Dataset Gambar untuk Percobaan

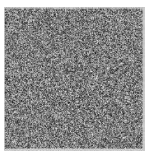
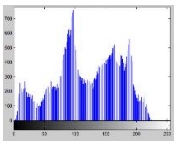
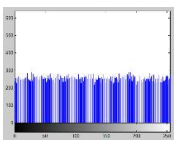
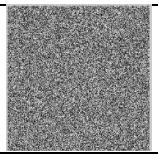
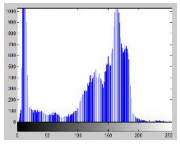
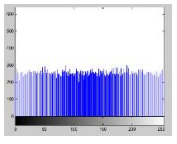
Uji evaluasi dilakukan dengan menganalisa hasil enkripsi dan dekripsi. Dalam makalah ini akan dianalisa pula nilai hasil eksperimen antara gambar berwarna dan gambar grayscale seperti pada Tabel 2.

Tabel 2. Evaluasi Hasil EnkripsiGambar Grayscale melalui Nilai MSE, PSNR dan BER

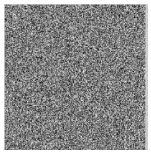
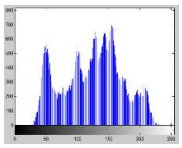
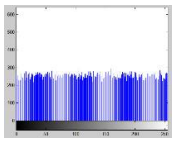
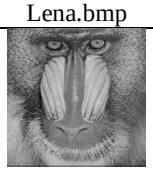
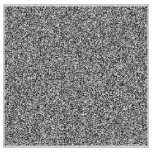
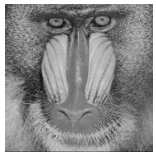
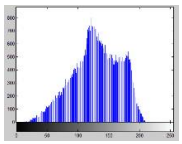
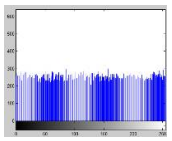
Nama Gambar	*Gambar Asli*	*MSE*	*PSNR (dB)*	*BER*
peppers.bmp		8384.7765	8.8959	26205
woman.bmp		9369.9172	7.4134	26230
lena.bmp		7712.9652	9.2586	26163
babbon.bmp		6954.4088	9.7082	26193

Berdasarkan Tabel 2, dapat dilihat bahwa proses enkripsi telah berhasil dengan pembuktian nilai PSNR dan BER. Nilai PSNR yang mula-mula di dapat dari nilai MSE, menghasilkan nilai mendekati 0. Dalam kriptografi, nilai PSNR yang rendah mengindikasikan hasil penyisipan data yang baik. Semakin rendah nilai PSNR maka semakin baik hasil enkripsi yang dihasilkan. Hal ini berbeda dengan teknik steganografi atau watermarking, dalam kedua teknik tersebut nilai PSNR yang dihasilkan harus lebih dari 30 dB. Untuk lebih jelas, perbandingan gambar enkripsi dan dekripsi telah disajikan pada Tabel 3 dengan tambahan hasil dalam bentuk histogram.

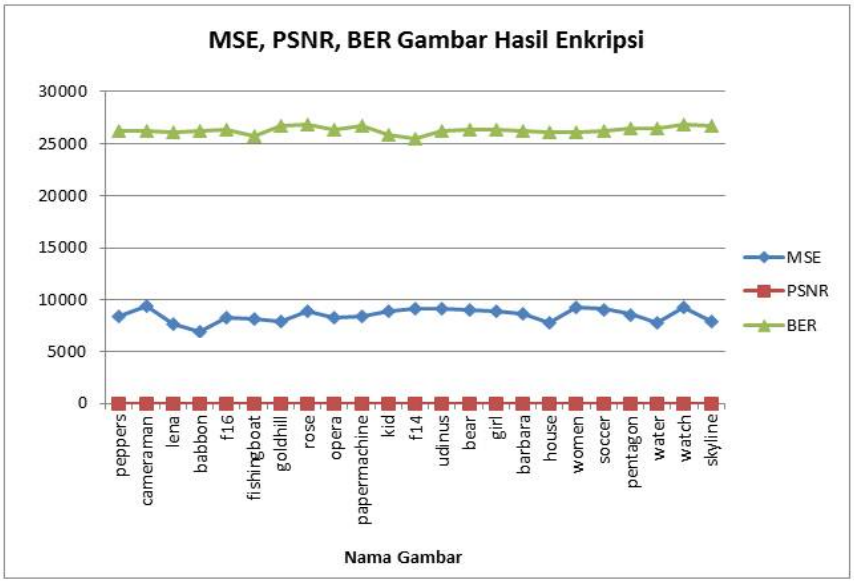
Tabel 3. Perbandingan Hasil Ekripsi pada Gambar Grayscale

Gambar Asli	*Gambar Hasil Enkripsi*	*Gambar Hasil Dekripsi*	*Histogram Gambar Asli*	*Histogram Gambar Hasil Enkripsi*
 Peppers.bmp				
				

ISBN: 9-789-7936-499-93

Cameraman.bmp				
 Lena.bmp				
 Baboon.bmp				

Eskperimen yang telah dilakukan menggunakan media citra grayscale telah menghasilkan nilai PSNR terbaik yaitu 8,4 dB. Nilai PSNR digunakan untuk membuktikan sejauh mana gambar tersebut tampak oleh mata manusia. Menurut Cheddad dalam penelitiannya menyebutkan bahwa pada teknik kriptografi terdapat kelemahan dalam aspek imperceptibility, hal ini dikarenakan operasi enkripsi biasanya merusak sebagian besar gambar (Cheddad, 2010). Sedangkan nilai BER pada proses enkripsi terbaik yaitu 26230. Nilai MSE, PSNR, dan BER pada 20 citra lainnya dapat dijabarkan pada Gambar 3, sedangkan hasil dekripsi dapat dilihat pada Gambar 4.

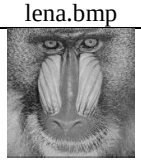


Gambar 3. Nilai MSE, PSNR, dan BER pada Hasil Enkripsi

Tabel 4. Evaluasi Hasil Dekripsi Gambar Grayscale melalui Nilai MSE, PSNR dan BER

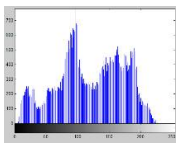
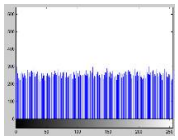
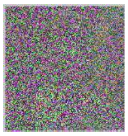
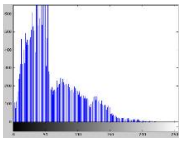
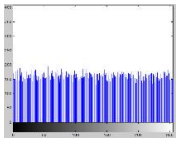
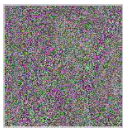
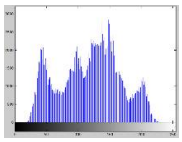
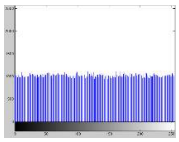
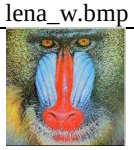
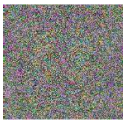
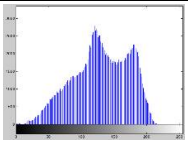
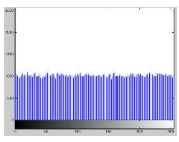
Gambar Asli	*MSE*	*PSNR (dB)*	*BER*
 peppers.bmp	0.0000	Inf	0.0000
 woman.bmp	0.0000	Inf	0.0000

ISBN: 9-789-7936-499-93

 lena.bmp	0.0000	Inf	0.0000
 babbon.bmp	0.0000	Inf	0.0000

Berdasarkan eksperimen yang telah dilakukan didapatkan hasil enkripsi dan dekripsi yang baik. Hasil enkripsi menunjukkan bahwa nilai MSE untuk semua gambar yaitu 0, dan PSNR yaitu inf, sedangkan BER yaitu 0. Dengan demikian terbukti bahwa gambar berhasil untuk dienkripsi dan didekripsi dengan baik, selanjutnya proses enkripsi dan dekripsi juga telah diuji coba menggunakan gambar berwarna sesuai Tabel 5.

Tabel 5. Perbandingan Hasil Ekripsi pada Gambar Warna

Gambar Asli	*Gambar Hasil Enkripsi*	*Gambar Hasil Dekripsi*	*Histogram Gambar Asli*	*Histogram Gambar Hasil Enkripsi*
 peppers_w.bmp				
 woman_w.bmp				
 lena_w.bmp				
 babbon_w.bmp				

Pada Tabel 5, dapat dilihat bahwa gambar berwarna setelah melalui proses enkripsi terbukti mempunyai bentuk histogram yang berbeda dengan gambar asli. Gambar hasil enkripsi menjadi tidak terdeteksi, dengan kata lain menjadi hancur seperti terkena *noise*.

10. KESIMPULAN

Dalam makalah ini, One Time Pad (OTP) telah berhasil diterapkan menggunakan gambar grayscale dan gambar berwarna berukuran 256x256 dengan format bmp. Dari 24 gambar yang digunakan untuk eksperimen, nilai PSNR untuk proses enkripsi terbaik yaitu 7,4134 dB, nilai BER terbaik yaitu 26230. Sedangkan pada proses dekripsi, nilai PSNR terbukti inf, BER dan MSE seluruh gambar yaitu 0. Hal ini membuktikan proses enkripsi dan dekripsi berjalan dengan baik. Untuk lebih menegaskan hasil enkripsi, dapat dilihat dari histogram gambar asli dan histogram hasil enkripsi.

PUSTAKA

Astuti, Y.P. et al., 2016. Optimasi Enkripsi Password Menggunakan Algoritma Blowfish. *Techno.COM*, 15(1), pp.15–21.

ISBN: 9-789-7936-499-93

Erawan, L. et al. 2017. Implementasi Kriptografi Simetris One Time Pad (OTP) pada File Dokumen. Seminar Nasional Budi Luhur. Universitas Budi Luhur. Jakarta.

Ignatius, D.R., Setiadi, M. & Rachmawanto, E.H., 2017. Secure Image Steganography Algorithm Based on DCT with OTP Encryption. *Journal of Applied Intelligent System*, 2(1), pp.1–11.

Jain, M. & Lenka, S.K., 2015. Secret data transmission using vital image steganography over transposition cipher. In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*. IEEE, pp. 1026–1029.

Jeyamala, C., GopiGanesh, S. & Raman, G.S., 2010. An image encryption scheme based on one time pads — A chaotic approach. In *2010 Second International conference on Computing, Communication and Networking Technologies*. IEEE, pp. 1–6. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5591643.

Li, J. et al., 2015. An image encryption method based on tent and Lorenz chaotic systems. In *2015 6th IEEE International Conference on Software Engineering and Service Science (ICSESS)*. IEEE, pp. 582–586. Available at: http://ieeexplore.ieee.org/document/7339125/.

Liansheng, S. et al., 2014. A novel grayscale image encryption algorithm based on logistic map. In *2014 International Conference on Information Science, Electronics and Electrical Engineering*. IEEE, pp. 222–225. Available at: http://ieeexplore.ieee.org/document/6948101/.

Munir, R., 2011. Enkripsi Selektif Citra Digital dengan Stream Cipher Berbasiskan pada Fungsi Chaotik Logistic Map. In *Seminar Nasional dan Expo Teknik Elektro 2011*. pp. 7–12.

Rachmawanto, E.H. & Sari, C.A., 2015. Keamanan File Menggunakan Teknik Kriptografi Shift Cipher. *Techno.COM*, 14(4), pp.329–335.[HYPERLINK "" \l "Era17" [1]]

Sari, C.A. et al., 2016. Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting. *Journal of Applied Intelligent System*, 1(3), pp.179–190.

Sari, C.A. & Rachmawanto, E.H., 2014. Gabungan Algoritma Vernam Chiper Dan End of File. *Techno.COM*, 13(3), pp.150–157.

Sekertekin, Y. & Atan, O., 2016. An image encryption algorithm using Ikeda and Henon chaotic maps. In *2016 24th Telecommunications Forum (TELFOR)*. IEEE, pp. 1–4. Available at: http://ieeexplore.ieee.org/document/7818872/.

Shukla, R. et al., 2013. Sampurna Suraksha: Unconditionally Secure and Authenticated One Time Pad Cryptosystem. In *2013 International Conference on Machine Intelligence and Research Advancement*. IEEE, pp. 174–178.

Tornea, O. et al., 2011. DNA Vernam Cipher. *Proceedings of the 3rd International Conference on E-Health and Bioengineering - EHB 2011*, pp.24–27.