Modifikasi Skema Teknik Tanam Padi dan Bajak Sawah Berbasis *Square Transposition 64-bit*

http://dx.doi.org/10.28932/jutisi.v7i1.2973
Riwayat Artikel
Received: 23 September 2020 | *Final Revision*: 15 Maret 2021 | *Accepted*: 24 Maret 2021

Nadya Glorya Najoan✉#1, Magdalena Ariance Ineke Pakereng*2

Jurusan Teknik Informatika, Universitas Kristen Satya Wacana
Jl. Dr. O. Notohamidjojo, Kel. Blotongan, Kec. Sidorejo, Salatiga
1najoannadya25@gmail.com

* *Jurusan Teknik Informatika, Universitas Kristen Satya Wacana*
Jl. Dr. O. Notohamidjojo, Kel. Blotongan, Kec. Sidorejo, Salatiga
2ineke.pakereng@uksw.edu

Abstract — **Cryptography is a study discussing mathematic technics that related to information security aspects such as secrecy, data integrity, and authenticity. This research discusses how to modify a scheme while looking for random points using different pickup points and income points. While looking for the random point in the modified scheme research using the rice planting and field plow techniques, it has three testing processes which were runtest, monobit, and blockbit tests. This research used square transpositions 64-bit with the size 8x8 and it got a high result with p-value 7.3239×10^{-10}, p-value monobit 1.00000000 and p-value blockbit 1 that showed non-random result with the smallest p-value was 0.011662392 with p-value monobit 1.00000000 and the p-value blockbit 0.99990476 that made this research got a random result.**

Keywords— **Blockbit; Cryptography; Monobit; Runtest; Square Transposition.**

I. PENDAHULUAN

Pada zaman modern seperti sekarang ini, perkembangan teknologi dan informasi sangat dibutuhkan oleh banyak orang. Hadirnya teknologi dan informasi, menyebabkan orang-orang bisa saling berkomunikasi walaupun dengan jarak yang sangat berjauhan. Internet merupakan salah satu hal yang bisa menghubungkan seseorang untuk berkomunikasi dan saling bertukar informasi dengan orang yang lain walaupun berada pada tempat yang berbeda. Beberapa orang ingin memberikan informasi untuk diberikan kepada pihak yang ditujunya dengan rahasia atau tanpa diketahui oleh orang lain. Berbagai carapun dilakukan supaya informasi yang akan diberikan tidak diketahui oleh pihak tidak berwenang sebelum sampai kepada pihak terkait. Maka dari itu kriptografi hadir untuk membantu mengamankan informasi dan data yang ada.

Kriptografi yang baik memiliki pola yang acak dan beragam[1], pola acak penting dalam kriptogtafi karena untuk menjadikan nilai tidak dapat diprediksi atau *unpredictable*[2], sehingga penelitian ini dirancang dengan menggunakan algoritma yang diterapkan dalam kriptografi yaitu algoritma *block cipher* 64-*bit* berbasis pada teknik tanam padi dan bajak sawah yang sudah diteliti sebelumnya[1], kemudian akan dimutasi nilai keacakannya pada tiga pengujian yaitu *runtest, monobit* dan *blockbit.*

Kendala yang ada pada penelitian sebelumnya telah diuji dengan menggunakan pola pengambilan dan pemasukan tanam padi dan bajak sawah dengan hasil yang didapatkan bernilai tidak acak, sehingga dilakukannya pengujian kembali dengan memodifikasi atau memperbaiki pola pengambilan dan pemasukan dari tanam padi dan bajak sawah sehingga memperoleh hasil yang bernilai acak.

Berdasarkan latar belakang yang ada maka dilakukan pengujian kembali dengan memodifikasi skema teknik tanam padi dan bajak sawah berbasis *square transposition 64-bit* sebagai pemenuhan nilai keacakan dari penelitian sebelumnya.

II. TINJAUAN PUSTAKA

Kriptografi sendiri adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi [3]. Kriptografi ini merupakan sebuah metode untuk mengamankan data maupun informasi dalam bentuk sandi sehingga tidak dapat dimengerti maknanya lagi. Melalui proses enkripsi dan dekripsi data atau pesan dapat diubah ke bentuk sandi dan memerlukan kunci untuk mengerti makna berdasarkan sandi tersebut. Namun bukan

jaminan data atau pesan menjadi aman ketika sudah diterapkan algoritma kriptografi di dalamnya karena seiring kemajuan kriptografi semakin banyak pula oknum-oknum yang ingin memecahkan algoritma tersebut [4].

Perancangan kriptografi *block cipher* yang dilakukan sekarang ini memerlukan penelitian yang telah dilakukan sebelumnya sehingga dapat digunakan sebagai dasar atau pembanding dari penelitian ini. Penelitian yang berjudul Modifikasi Skema Teknik Tanam Padi dan Bajak Sawah Berbasis *Square Transposition 64-bit* sebagai Pemenuhan Nilai Keacakan adalah acuan dari penelitian ini dimana pada proses tanam padi dilakukan proses menaruh bibit padi pada sebidang tanah yang membentuk aturan pola tertentu agar dapat tumbuh dengan baik. Proses tanam padi ini membentuk alur horizontal dan vertikal yang saling berkesinambungan. Proses dalam menaruh bibit padi dengan memasukkan bibit padi sekitar 5 cm ke dalam tanah, setelah terisi mundur ke belakang sesuai petakan sawah. Sedangkan Proses bajak sawah sendiri adalah mengerjakan tanah dengan menggunakan alat yang disebut bajak. Tujuan dari membajak tersebut yaitu dengan membalikkan tanah yang sebelumnya ada di lapisan paling atas sudah ditumbuhi rumput dan cenderung lebih keras, maka dengan proses dibajak lapisan tanah di bawahnya naik ke atas dan menjadi lebih gembur. Proses bajak sawah menggunakan pola spiral dimulai dari titik terluar atau pinggur, setelah itu memutar mengelilingi titik pusat [1].

Run Test dapat digunakan untuk melihat apakah observasi (sampel) diambil secara acak atau tidak. Barisan yang dilakukan pengujian menggunakan *run test* dapat berupa uji biner maupun uji non-biner. Pada penelitian ini dilakukan strategi penerapan untuk melakukan uji keacakan barisan *bit* menggunakan *run test* [5]. Dalam pengujian ini mencari jumlah total lintasan dalam suatu rangkaian, dimana lintasan adalah rangkaian tak berujung dari *bit* yang identik. Tujuan dari percobaan lintasan ini untuk menentukan jumlah lintasan satu dan nol dalam berbagai jarak untuk suatu rangkaian yang acak. Secara khusus, percobaan ini menentukan apakah pergerakan antara nol dan satu terlalu cepat atau terlalu lambat Panjang lintasan *k* terdiri dari *bit k* yang identik dan dibatasi sebelum dan sesudah oleh suatu *bit* dengan nilai yang berlawanan, nilai berlawanan yang dimaksud jika value 0 atau 1 sudah di input sebelumnya maka nilai berlawanannya yang di input 1 atau 0. [6].

Monobit Test adalah pengujian untuk menentukan apakah jumlah satu dan nol dalam suatu rangkaian kurang lebih sama dengan yang akan diperkirakan terhadap suatu rangkaian yang benar-benar acak. Percobaan ini memperhitungkan pendekatan suatu fraksi atau pecahan dari satu sampai setengah, itulah jumlah dari satu dan nol dalam suatu rangkaian yang seharusnya sama [6].

Blockbit Test adalah percobaan untuk menentukan apakah frekuensi dari satu dalam suatu balok *M-bit* adalah kurang lebih M/2, sama seperti yang akan diharapkan dalam suatu perkiraan yang acak. Untuk balok berukuran M=1, percobaan ini merosot kembali ke percobaan 1, yaitu percobaan Frekuensi *Monobit*[6].

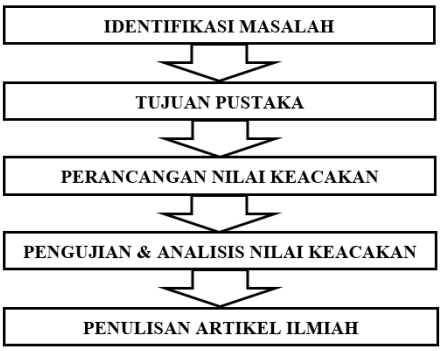
Square Transposition merupakan salah satu jenis dari transposisi *cipher*. *Square Transposition* sendiri dapat digunakan dengan aman apabla kunci yang digunakan cukup panjang[7]. *Square Transposition* sendiri terdiri dari dua proses yaitu memasukka *bit* ke dalam *square* dan proses pengambilan *bit* dengan ukuran yang telah ditentukan sebelumnya[8].

Batik Bentenan merupakan kain batik traditional hasil karya Suku Minahasa yang ada sekitar abad ke-7 [9]. Motif Batik Bentenan yang digunakan pada penelitian ini adalah motif dari kain Tinompak yaitu motif yang berarti muncul atau memunculkan simbol-simbol selain simbol manusia *(human figure)*, misalnya menambahkan motif pakis hutan *(flora)* dan motif ekor ikan *(fauna)*[10]. Motif Tinompak juga adalah salah satu teknik tenunan dengan aneka pola dengan gambar yang berulang[11].

Pengujian Nilai Keacakan dilakukan untuk melihat seberapa baik rancangan kriptografi mengacak nilai *plaintext*. Nilai keacakan sendiri dilihat dapat dilihat dari selisih perbandingan *plaintext* dengan *cyphertext* terhadap *plaintext* karena selisih pada pembilang, pada persamaan dengan kemungkinan yang muncul pada nilai keacakan dapat bernilai positif maupun negatif. Apabila mendapatkan nilai negatif berarti perbandingan nilai *cyphertext* lebih besar dari nilai *plaintext* begitu juga sebaliknya apabila mendapatkan nilai positif berarti nilai *plaintext* lebih besar dari nilai *cyphertext* [12].

III. METODE PENELITIAN

Tahapan penelitian ini terdiri dari 4 (empat) tahapan, yaitu: (1). Identifikasi masalah, (2). Tinjauan Pustaka, (3). Pengujian Nilai Keacakan dan Analisa (4). Penulisan Artikel Ilmiah



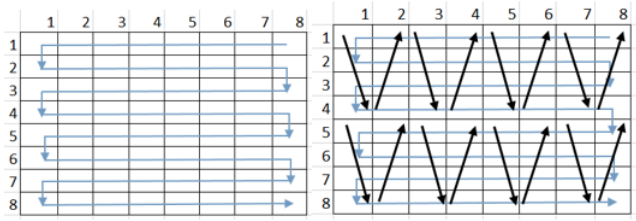
Gambar 1. Tahapan Penelitian

Tahapan penelitian pada Gambar 1 dapat dijelaskan sebagai berikut:

Tahap pertama: Identifikasi masalah merupakan tahap awal untuk mencari permasalahan dari nilai yang tidak acak

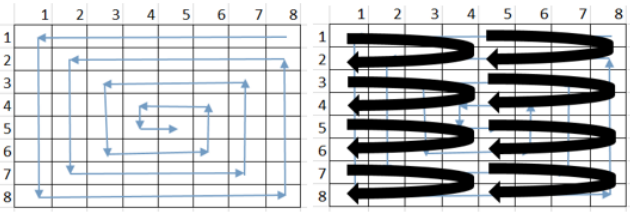
menjadi acak atau dengan kata lain penelitian tentang *Pseudo Random Number Generator* dengan Modifikasi Skema Teknik Tanam Padi dan Bajak Sawah Berbasis *Square Transposition 64-bit* sebagai Pemenenuhan Nilai Keacakan yang berkaitan dengan Modifikasi Skema Teknik Tanam Padi dan Bajak Sawah Berbasis *Square Transposition 64-bit* sebagai Pemenenuhan Nilai Keacakan; Tahap kedua: Tinjauan pustaka dilakukan dengan mengumpulkan referensi dari buku, jurnal atau sumber lain yang berguna dalam perancangan kriptografi; Tahapan ketiga: Perancangan Nilai Keacakan pada Skema Teknik Tanam Padi dan Bajak Sawah Berbasis *Square Transposition 64-bit* sebagai Pemenuhan Nilai Keacakan; Tahapan keempat: Pengujian dan analisa Nilai Keacakan pada Modifikasi Skema Teknik Tanam Padi dan Bajak Sawah Berbasis *Square Transposition 64-bit* sebagai Pemenuhan Nilai Keacakan. Penulisan laporan dari hasil penelitian yang dilakukan mengenai proses Modifikasi Skema Teknik Tanam Padi dan Bajak Sawah Berbasis *Square Transposition 64-bit* sebagai Pemenuhan Nilai Keacakan.

Dalam memodifikasi skema teknik tanam padi dan bajak sawah berbasis *square transposition* dilakukan dua proses yaitu pola pengambilan dan pola pemasukan.



Gambar 2. Pola Pengambilan Zig-zag dan Pola Pemasukan Tanam Padi

Dalam pengujian ini adalah menggunakan pola pengambilan zig-zag dan pemasukan menggunakan pola tanam padi yang dibagi menjadi dua bagian yaitu bagian atas dan bagian bawah. Setelah itu pemasukan dimulai dari bagian atas samping kiri mengikuti arah panah ke bagian bawah empat karakter dan ke kanan satu karakter setelah itu naik ke bagian atas tiga karakter mengikuti arah panah dilakukan dengan cara yang sama untuk bagian bawah seperti pada Gambar 2 [4].



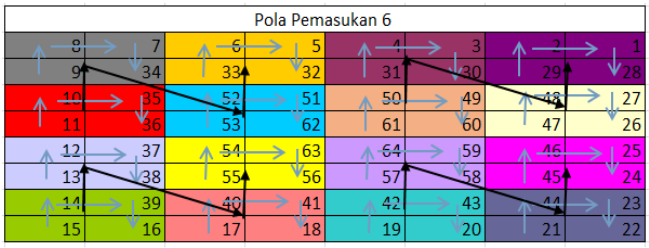
Gambar 3. Pola Pengambilan Spiral dan Pola Pemasukan Bajak Sawah

Dalam pengujian menggunakan pola pengambilan spiral dan pola pemasukan bajak sawah dimulai dari pengambilan dari samping kanan atas dan pemasukan dari samping kiri atas maju ke kanan 4 karakter kemudian berurutan ke bawah ke kiri empat karakter mengikuti arah anak panah pada Gambar 3 [4].

IV. HASIL DAN PEMBAHASAN

Dalam bagian ini akan membahas mengenai Modifikasi Skema Teknik Tanam Padi dan Bajak Sawah Berbasis *Square Transposition 64-bit* sebagai Pemenuhan Nilai Keacakan secara terinci.

Proses pertama dalam mencari nilai keacakan dengan menggunakan pola pengambilan spiral dan pemasukan bajak sawah mendapatkan hasil yang acak seperti pada Gambar 4.



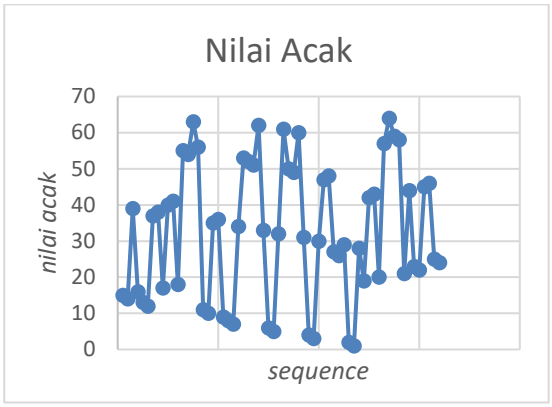
Gambar 4 Pola Spiral dan Bajak Sawah

Dalam mencari nilai keacakan dengan menggunakan pola spiral dan bajak sawah diperlukan enam kali proses. Terlihat pada Gambar 4 dipisahkan menjadi empat bagian yaitu sisi kiri bawah, sisi kiri atas , sisi kanan bawah dan sisi kanan atas. Pengambilan dimulai dari pojok kiri bawah dengan pemakaian empat karakter (15) setelah itu keatas (38) dan turun kembali ke bawah dan naik kembali ke atas dengan mengikuti arah anak panah sehingga membentuk huruf *N* dengan hasil menggunakan 16 karakter dalam satu sisi tersebut. Begitu juga untuk sisi kiri atas, sisi kanan bawah dan sisi kanan atas dilakukan dengan hal yang sama sehingga pengambilan membentuk huruf *N* (28) dengan mengikuti arah anak panah yang ada.

Proses dengan pengujian enam kali putaran untuk mendapatkan nilai keacakan:

1. {15, 14, 39, 16, 13, 12, 37, 38, 17, 40, 41, 18, 55, 54, 63, 56}
2. {11, 10, 35, 36, 9, 8, 7, 34, 53, 52, 51, 62, 33, 6, 5, 32}
3. {19, 42, 43, 20, 57, 64, 59, 58, 21, 44, 23, 22 , 45, 46, 25, 24 }
4. {61, 50, 49, 60, 31, 1, 3, 30, 47, 48, 27, 26, 29, 2, 1, 28}

p-ISSN : 2443-2210
e-ISSN : 2443-2229



Gambar 5. Grafik Keacakan pada Pola Spiral dan Bajak Sawah

Dengan nilai-nilai keacakan tersebut membentuk grafik keacakan berasal dari pola pengambilan spiral dan pola pemasukan bajak sawah seperti pada Gambar 5.

TABEL I
HASIL PENGUJIAN PENGAMBILAN SPIRAL DAN PEMASUKAN BAJAK SAWAH

Pengujian	*Runtest*	*Monobit*	*Blockbit*	Hasil
Pengujian 1	2.76369×10^{-5}	1.00000000	1	Tidak Acak
Pengujian 2	2.86459×10^{-6}	1.00000000	0.99999933	Tidak Acak
Pengujian 3	2.3257×10^{-7}	1.00000000	1	Tidak Acak
Pengujian 4	2.3257×10^{-7}	1.00000000	1	Tidak Acak
Pengujian 5	0.00124688	1.00000000	1	Tidak Acak
Pengujian 6	0.021896615	1.00000000	0.756404451	Tidak Acak

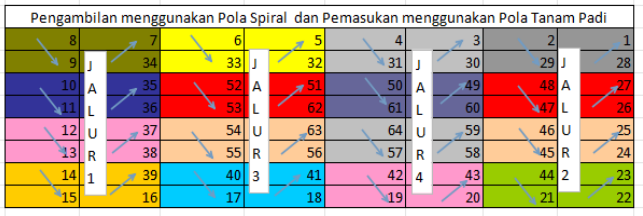
Tabel I adalah hasil dari enam kali percobaan pengujian untuk mendapatkan nilai keacakan dalam pola pengambilan spiral dan pola pemasukan bajak sawah dan mendapatkan nilai keacakan pada pengujian yang keenam dengan nilai *runtest* 0.021896615, nilai *monobit* 1.0000000 dan nilai *blockbit* 0.756404451.

Gambar 6 adalah hasil dari perhitungan untuk mencari nilai keacakan pada pola spiral dan bajak sawah.

runtest	
mean=	32,5
R=	25
n0=	32
n1=	32
n=	64
E(R)=	33,000
Var(R)=	15,746
StDev(R)=	3,968
Z=	-2,016
p-value=	0,02189662
α=	0,01
Hasil	ACAK

Gambar 6. Perhitungan Nilai Keacakan pada Pola Spiral dan Bajak Sawah

Hasil acak atau tidak acak didapatkan jika *p-value* kurang dari *α-value*, maka hasilnya tidak acak, karena pada hasil ini didapatkan nilai *p-value* lebih besar dari nilai *a-value* maka menghasilkan nilai acak.

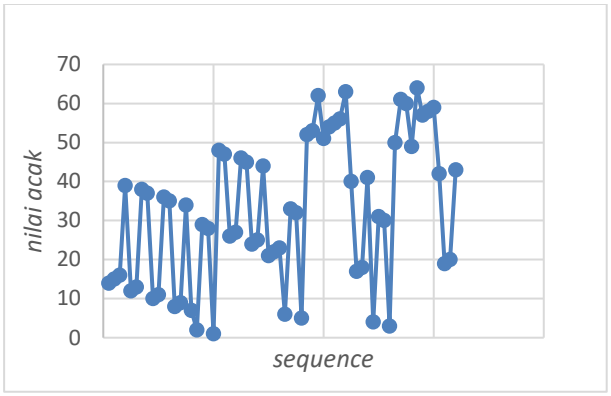


Gambar 7. Pola Spiral dan Tanam Padi

Dalam mencari nilai keacakan Gambar 7 dengan menggunakan pola pengambilan spiral dan pola pemasukan menggunakan tanam padi dibagi menjadi empat jalur yaitu jalur satu, jalur dua, jalur tiga dan jalur empat dimana jalur satu dan jalur tiga bersebelahan dissmping kiri sedangkan jalur dua dan jalur empat berada pada posisi samping kanan bersebelahan. Pengujian dimulai dari jalur satu samping kiri paling atas (8) dan mengikuti arah anak panah menurun ke bawah sampai akhir jalur satu (39). Selanjutnya pengujian pada jalur ke dua dengan pengambilan dimulai dari samping kanan bagian atas (2) mengukuti arah panah dan menuju ke arah bawah (23). Untuk jalur tiga dan jalur empat dilakukan pengujian seperti pada jalur satu dan jalur dua.

Proses dengan menggunakan pola pengambilan spiral dan pemasukan tanam padi terdapat tujuh kali pengujian mendapat nilai keacakan:

1. {8, 9, 7, 34, 10, 11, 36, 35, 12, 13, 37, 38, 14, 15, 39, 16}
2. {2, 29, 28, 1, 48, 47, 26, 27, 46, 45, 24, 25, 44, 21, 22, 23}
3. {6, 33, 32, 5, 52, 53, 62, 51, 54, 55, 56, 63, 40, 17, 18, 41}
4. {4, 31, 30, 3, 50, 61, 60, 49, 64, 57, 58,59 ,42, 19, 20, 43}



Gambar 8. Grafik Keacakan pada Pola Spiral dan Tanam Padi

Gambar 8 merupakan grafik keacakan nilai-nilai yang telah diuji dengan menggunakan pola pengambilan spiral dan pola pemasukan tanam padi.

TABEL II
HASIL PENGUJIAN PENGAMBILAN SPIRAL DAN PEMASUKAN TANAM PADI

Pengujian	*Runtest*	*Monobit*	*Blockbit*	Hasil
Pengujian 1	0.001246883	1.00000000	0.999707663	Tidak Acak
Pengujian 2	2.3257×10^{-7}	1.00000000	1	Tidak Acak
Pengujian 3	2.86459×10^{-6}	1.00000000	1	Tidak Acak
Pengujian 4	0.001246883	1.00000000	1	Tidak Acak
Pengujian 5	0.002784893	1.00000000	0.999970476	Tidak Acak
Pengujian 6	0.000209267	1.00000000	0.966491465	Tidak Acak
Pengujian 7	0.011662392	1.00000000	0.999904763	Acak

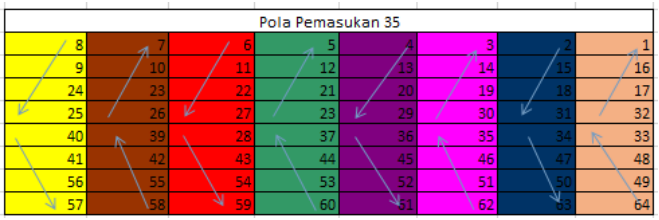
Pada Tabel II adalah hasil dari tujuh kali proses percobaan untuk mencari nilai keacakan dengan menggunakan pola pengambilan spiral dan pola pemasukan tanam padi yang akhirnya pada pengujian ketujuh mendapatkan nilai acak dengan *runtest* 0.011662392, nilai *monobit* 1.0000000 dan mendapatkan nilai *blockbit* 0.999904763.

Gambar 9 adalah hasil dari perhitungan untuk mencari nilai keacakan pada pola spiral dan tanam padi.

runtest	
mean=	32,5
R=	24
n0=	32
n1=	32
n=	64
E(R)=	33,000
Var(R)=	15,746
StDev(R)=	3,968
Z=	-2,268
p-value=	0,011662392
α=	0,01
Hasil	ACAK

Gambar 9. Perhitungan Nilai Keacakan pada Pola Spiral dan Tanam Padi

Hasil acak atau tidak acak didapatkan jika *p-value* kurang dari *α-value*, maka hasilnya tidak acak, karena pada hasil ini didapatkan nilai *p-value* lebih besar dari nilai *a-value* maka menghasilkan nilai acak.



Gambar 10. Pola Zig-zag dan Tanam Padi

Pada Gambar 10 terdapat delapan sisi pada saat mencari nilai keacakan. Terdapat 35 kali percobaan untuk mencari nilai kecakan pada pola pengambilan zig-zag dan pola pemasukan tanam padi. Pencarian nilai keacakan dimulai dari mengambil angka paling kanan bawah (64) dengan melanjutkan ke atas sesuai arah anak panah sampai pada pojok kanan atas (1) dan kemudian lakukan juga kepada sisi ketujuh lainnya dengan arah naik-turun seperti arah anak panah dan berakhir pada kolom kiri bagian bawah (57).

Dalam pecarian nilai keacakan pada pola pengambilan zig-zag dan pola pemasukan tanam padi untuk pengujian *monobit* dan *blockbit* mendapatkan nilai yang acak sedangkan pengujian *runtest* tidak mendapatkan nilai yang acak sehingga harus dilakukan kembali pencarian nilai keacakan dengan menggunakan pola baru.

p-ISSN : 2443-2210
e-ISSN : 2443-2229

TABEL III
HASIL PENGUJIAN PENGAMBILAN ZIG-ZAG DAN PEMASUKAN TANAM PADI

Pengujian	*Runtest*	*Monobit*	*Block Bit*	Hasil
Pengujian 1	2.8088×10^{-15}	1.00000000	1	Tidak Acak
Pengujian 2	7.32395×10^{-10}	1.00000000	1	Tidak Acak
Pengujian 3	2.8088×10^{-15}	1.00000000	1	Tidak Acak
Pengujian 4	1.48629×10^{-10}	1.00000000	1	Tidak Acak
Pengujian 5	8.6082×10^{-13}	1.00000000	1	Tidak Acak
Pengujian 6	1.35338×10^{-13}	1.00000000	1	Tidak Acak
Pengujian 7	1.48629×10^{-10}	1.00000000	1	Tidak Acak
Pengujian 8	1.3533×10^{-13}	1.00000000	1	Tidak Acak
Pengujian 9	5.11981×10^{-12}	0.72367361	1	Tidak Acak
Pengujian 10	3.39201×10^{-9}	1.00000000	1	Tidak Acak
Pengujian 11	2.83459×10^{-11}	1.00000000	1	Tidak Acak
Pengujian 12	3.39201×10^{-9}	1.00000000	1	Tidak Acak
Pengujian 13	7.32395×10^{-10}	1.00000000	1	Tidak Acak
Pengujian 14	2.3257×10^{-7}	1.00000000	1	Tidak Acak
Pengujian 15	1.48629×10^{-10}	1.00000000	1	Tidak Acak
Pengujian 16	1.48629×10^{-10}	1.00000000	1	Tidak Acak
Pengujian 17	3.39201×10^{-9}	1.00000000	1	Tidak Acak
Pengujian 18	2.3257×10^{-7}	1.00000000	1	Tidak Acak
Pengujian 19	2.8088×10^{-15}	1.00000000	1	Tidak Acak
Pengujian 20	3.39201×10^{-9}	1.00000000	1	Tidak Acak
Pengujian 21	3.392×10^{-9}	1.00000000	1	Tidak Acak
Pengujian 22	6.04369×10^{-8}	1.00000000	1	Tidak Acak
Pengujian 23	1.4767×10^{-8}	1.00000000	1	Tidak Acak
Pengujian 24	1.35338×10^{-13}	1.00000000	1	Tidak Acak
Pengujian 25	1.48629×10^{-10}	1.00000000	1	Tidak Acak
Pengujian 26	1.48629×10^{-10}	1.00000000	1	Tidak Acak
Pengujian 27	2.83459×10^{-11}	1.00000000	1	Tidak Acak
Pengujian 28	3.39201×10^{-9}	1.00000000	1	Tidak Acak
Pengujian 29	1.35338×10^{-13}	1.00000000	1	Tidak Acak
Pengujian 30	1.4767×10^{-8}	1.00000000	1	Tidak Acak
Pengujian 31	9.17249×10^{-6}	1.00000000	1	Tidak Acak
Pengujian 32	2.8088×10^{-15}	1.00000000	1	Tidak Acak
Pengujian 33	6.04369×10^{-8}	1.00000000	1	Tidak Acak
Pengujian 34	3.39201×10^{-9}	1.00000000	1	Tidak Acak
Pengujian 35	7.32395×10^{-10}	1.00000000	1	Tidak Acak

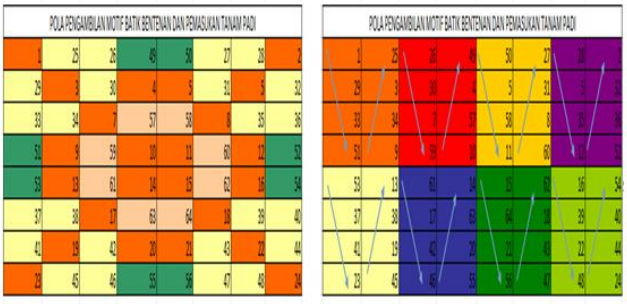
Dalam melakukan pengujian nilai keacakan pada Pola pengambilan zig-zag dan pola pemasukan tanam padi tidak mendapatkan nilai keacakan seperti pada Tabel III, maka dari itu dilakukannya percobaan dengan menggunakan pola baru yaitu pola motif batik bentenan dan pola pemasukan tanam padi.

Gambar 11 adalah hasil dari perhitungan untuk mencari nilai keacakan pada pola zig-zag dan tanam padi.

runtest	
mean=	32,5
R=	9
n0=	32
n1=	32
n=	64
E(R)=	33,000
Var(R)=	15,746
StDev(R)=	3,968
Z=	-6,048
p-value=	7,3239E-10
α=	0,01
Hasil	TIDAK ACAK

Gambar 11. Perhitungan Nilai Keacakan pada Pola Zig-zag dan Tanam Padi

Hasil acak atau tidak acak didapatkan jika *p-value* kurang dari *α-value*, maka hasilnya tidak acak, karena pada hasil ini didapatkan nilai *a-value* lebih besar dari nilai *p-value* maka menghasilkan nilai tidak acak.

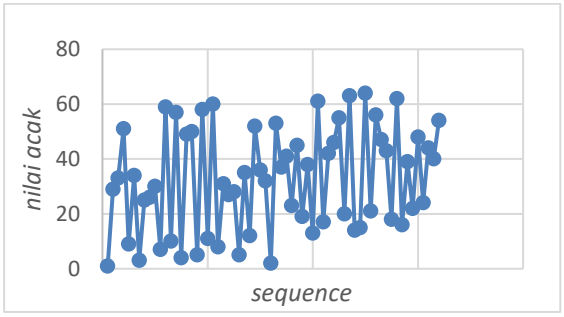


Gambar 12. Pola Motif Batik Bentenan dan Tanam Padi

Pada percobaan kali ini dengan menggunakan pola pemasukan baru motif batik bentenan dan pola pemasukan tanam padi sebagai salah satu pengujian untuk mendapatkan nilai keacakan. Gambar 12 memiliki dua gambar yaitu gambar disebelah kiri adalah pola motif batik bentenan sendiri dan gambar disebelah kanan adalah pencarian nilai keacakan dari pola tersebut. Pencarian nilai keacakan pada gambar sebelah kanan dibagi menjadi dua bagian yaitu bagian atas dan bagian bawah. Pengambilan awal dimulai dari bagian atas samping kiri (1) dan mengikuti arah anak panah dengan empat karakter berjejeran ke bawah atau ke atas sampai pada pojok kanan (2) dan untuk bagian bawah dilakukan hal yang sama seperti pada bagian yang diatas dari sebelah kiri bawah (53) sampai dengan bagian kanan bawah (54).

Proses pengambilan pola motif batik bentenan dan pemasukan tanam pagi hanya perlu dilakukan satu kali pengujian hingga mendapatkan nilai keacakan:

1. {1, 29, 33, 51, 9, 34, 3, 25, 26, 30, 7, 59, 10, 57, 4, 49}
2. {50, 5, 58, 11, 60, 8, 31, 27, 28, 5, 35, 12, 52, 36, 32, 2}
3. {53, 37, 41, 23, 45, 19, 38, 13, 61, 17, 42, 46, 55, 20, 63, 14}
4. {15, 64, 21, 56, 47, 43, 18, 62, 16, 39, 22, 48, 24, 44, 40, 54}



Gambar 13. Grafik Keacakan pada Pola Motif Batik Bentenan dan Tanam Padi

Gambar 13 merupakan grafik keacakan nilai-nilai yang telah diuji dengan menggunakan pola pengambilan pola motif batik bentenan dan pola pemasukan tanam padi.

TABEL IV
HASIL PENGUJIAN PENGAMBILAN MOTIF BATIK BENTENAN DAN PEMASUKAN TANAM PADI

Pengujian	*Runtest*	*Monobit*	*Blockbit*	Hasil
Pengujian 1	0.988337608	1.00000000	0.999707663	Acak

Tabel IV adalah hasil akhir dari pencarian nilai keacakan pada pola pengambilan motif batik bentenan dan pola pemasukan tanam padi dengan nilai *runtest* 0.988337608, nilai *monobdit* 1.00000000 dan mendapatkan nilai *blockbit* 0.999707663

Pada pencarian nilai keacakan dengan menguji pola pengambilan zig-zag dan pola pemasukan tanam padi mendapatkan hasil tidak acak dikarenakan pemasukan angka dengan alur zig-zag bersifat berurutan sehingga pada saat dilakukannya pengujian dengan pola tanam padi secara vertikal maupun horizontal tidak bisa mendapatkan nilai keacakan. Sedangkan dengan pengujian menggunakan pola pengambilan motif batik bentenan dan pola pemasukan tanam padi mendapatkan nilai acak dikarenakan pemasukan angka pada pola motif batik bentenan tersebut tidak berurutan sehingga pada saat pengujian dengan pola tanam padi secara vertikal maupun horizontal mendapatkan nilai acak sehingga pengujian nilai keacakan terpenuhi.

Gambar 14 adalah hasil dari perhitungan untuk mencari nilai keacakan pada pola motif Batik Bentenan dan tanam padi.

runtest	
mean=	32,484375
R=	42
n0=	32
n1=	32
n=	64
E(R)=	33,000
Var(R)=	15,746
StDev(R)=	3,968
Z=	2,268
p-value=	0,988337608
α=	0,01
Hasil	ACAK

Gambar 14. Perhitungan Nilai Keacakan pada Pola Motif Batik Bentenan dan Tanam Padi

Hasil acak atau tidak acak didapatkan jika *p-value* kurang dari *α-value*, maka hasilnya tidak acak, karena pada hasil ini didapatkan nilai *p-value* lebih besar dari nilai *a-value* maka menghasilkan nilai acak.

TABEL V
HASIL PENELITIAN POLA PENGAMBILAN DAN PEMASUKAN SEBELUM MODIFIKASI

No	Pengambilan dan Pemasukan	*p-value*			Hasil
		Run Test	*Mono Bit*	*Block Bit*	
1.	Pola Pengambilan Spiral & Pemasukan Bajak Sawah	2.76369×10^{-5}	1.00000000	1	Tidak Acak
2.	Pola Pengambilan Spiral & Pemasukan Tanam Padi	0.012469	1.00000000	0.99970766 3	Tidak Acak
3.	Pola Pengambilan Spiral & Pemasukan Tanam Padi	2.8088×10^{-15}	1.00000000	1	Tidak Acak

Tabel V dalah hasil dari setiap penelitian awal yang belum dimodifikasi polanya, sehingga mendapatkan nilai yang tidak acak dalam pengujian *runtest*, *monobit* dan *blockbit*.

TABEL VI
HASIL PENELITIAN POLA PENGAMBILAN DAN PEMASUKAN SETELAH MODIFIKASI

No	Pengambilan dan Pemasukan	*p-value*			Hasil
		Run Test	*Mono Bit*	*Block Bit*	
1.	Pola Pengambilan Spiral & Pemasukan Bajak Sawah	0.021896615	1.000000 00	0.7564 04451	Acak
2.	Pola Pengambilan Spiral & Pemasukan Tanam Padi	0.011662 392	1.000000 00	0.9999 0476	Acak
3.	Pola Pengambilan Zig-zag & Pemasukan Tanam Padi	7.32395×10^{-10}	1.000000 00	1	Tidak Acak
4.	Pola Pemasukan Motif Batik Bentenan dan Pengambilan Tanam Padi	0.988337 608	1.000000 00	0.9997 07663	Acak

Tabel VI adalah hasil dari setiap penelitian yang sudah diuji kembali dengan pola pengambilan dengan pola pemasukan. Berdasarkan dari empat data yang sudah diperoleh maka nilai *p-value* terbesar adalah *runtest* 7.3239×10^{-10} dengan nilai *p-value monobit* 1.00000000 dan nilai *p-value blockbit* 1 sehingga mendapatkan hasil tidak acak dan nilai *p-value* terkecil yaitu 0.011662392 dengan nilai *p-value monobit* 1.00000000 dan nilai *p-value blockbit* adalah 0.99990476 sehingga pengujian ini mendapatkan hasil acak.

V. SIMPULAN

Berdasarkan perancangan yang telah dibuat dapat disimpulkan bahwa Modifikasi Skema Teknik Tanam Padi dan Bajak Sawah Berbasis S*quare Transposition 64-bit* sebagai Pemdenuhan Nilai Keacakan dapat dikatakan acak apabila pengujian tersebut tidak bersifat berurutan pada saat dimasukan kedalam *square transposition 64-bit* berukuran 8x8. Maka dari itu pola pengambilan zig-zag tidak disarankan untuk dipakai pada saat akan mencari nilai keacakan dikarenakan akan mendapatkan hasil tidak acak.

Dari hasil perbandigan setiap pengujian menggunakan pola pengambilan dan pola pemasukan didapatkan nilai *p-value* terbesar adalah *runtest* 7.32395×10^{-10} dengan nilai *p-value monobit* 1.00000000 dan nilai *p-value blockbit* 1 sehingga mendapatkan hasil tidak acak dan nilai *p-value* terkecil yaitu 0.011662392 dengan nilai *p-value monobit* 1.00000000 dan nilai *p-value blockbit* adalah 0.99990476 sehingga pengujian ini mendapatkan hasil acak.

UCAPAN TERIMA KASIH

Terima kasih saya ucapkan kepada Pembimbing saya Ibu. Magdalena A. Ineke Pakereng yang dan Reviewer saya Bapak Alz D. Wowor yang sudah membantu dan membimbing saya sehingga penelitian ini bisa selesai.

DAFTAR PUSTAKA

[1] A. Widodo, A. D. Wowor, E. Mailoa, and M. A. I. Pakereng, "Perancangan Kriptografi Block Cipher Berbasis pada Teknik Tanam Padi dan Bajak Sawah," Salatiga, pp. 2–7, 2015.

[2] Bruce Schneier,*Applied Cryptography*,*Protocols*,*Algorithms & Source Code in C, 20th Anniversary Edition*, 2015, Wiley, page 45.

[3] N. D. Nathasia and A. E. Wicaksono, "Penerapan Teknik Kriptografi Stream-Cipher Untuk Pengaman Basis Data," *ICT Research Center UNAS*, Jurnal Basis Data, Jakarta Selatan, vol. 6, 2011.

[4] A. D. Wowor, M. A. I. Pakereng, F. Tuhumury, and A. D. Wowor, *"Perancangan Kriptografi Block Cipher 256 Bit Berbasis pada Pola Tuangan Air."* Jurusan Teknik Informatika Universitas Kristen Satya Wacana, Salatiga, 2016.

[5] I. M. M. K. Astawa, "Strategi Penerapan Uji Keacakan Barisan Bit Menggunakan Uji Run," vol. 1, no. 1, 2014.

[6] A. Rukhin, J. Soto, and J. Nechvatal, *"A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,"* April, 2010.

[7] D. Sinaga and C. Umam, *"Implementasi kriptografi vigenere cipher pada media teks dengan kombinasi transposisi kolom 1,2,"* Pros. SENDI_U 2018 ISBN 978-979-3649-99-3, no. 1, pp. 978–979, 2018.

[8] M. A. I. Pekereng and A. D. Wowor, *"Square Transposition : Suatu Pendekatan Proses Transposisi dalam Block Cipher,"* vol. x, no. x, pp. 1–8, 2018, doi: 10.11591/eei.vxix.yyyy.

[9] A. P. Tololiu, "Perlindungan Hukum Terhadap Kain Bentenan Sebagai Ekspresi Budaya Tradisional Sulawesi Utara," vol. 2, no. 2, pp. 1–12, 2014.

[10] A. F. Lowis, A. P. K, R. P. Sutanto, and J. Siwalankerto, "Perancangan Fotografi Esai Tentang Peran Masyarakat Manado dalam Mengapresiasi Kain Tenun Bentenan," vol. 1, no. 14, 2019.

[11] D. P. S. Hum, B. Agus, S. S. Iip, and A. P. Manangkalangi, "Perancangan Typeface Latin Hasil Adaptasi Budaya Suku Minahasa," Fti Umn, vol. 53, no. 9, pp. 1–15, 2018.

[12] S. H. Yonatan, H. D. Purnomo, and A. D. Wowor, "Perancangan Kriptografi Block Cipher Berbasis pada Garis Pertumbuhan dan Pita Pertumbuhan Cangkang Kerang," Salatiga, 2015. [Online]. Tersedia: https://repository.uksw.edu/handle/123456789/15079.