AIP Conference Proceedings

scitation.org/journal/apc

Volume 2391

International Conference on Science and Applied Science (ICSAS) 2021

Surakarta, Indonesia • 6 April 2021

Editors • Budi Purnama, Dewanta Arya Nugraha and A Suparmi

ICSAS 2021

International Conference on Science and Applied Science 2021

AIP Publishing

Preface: International Conference On Science And Applied Science (ICSAS) 2021

International Conference on Science and Applied Science (ICSAS) 2021 was the sixth conference which was organized by the Physics Department, Universitas Sebelas Maret. On this occasion, the ICSAS 2021 was held virtually on April 6th, 2021, due to the COVID-19 pandemic. The ICSAS 2021 conference is aimed to bring together scholars, leading researchers, and experts from diverse backgrounds and application areas in science. Special emphasis is placed on promoting interaction between the science theoretical, experimental, and other topics related to physics.

In ICSAS 2021, there are 8 parallel sessions and four keynote speakers. The keynote speakers provided to talk about the current research such as the application of multiferroic material for high speed devices; following the second keynote were speaker talk the magnetic-interaction of the interlayer systems in nanometer order. Other keynote speaker provided to talk solution of Klein Gordon equation coupled directly by quadratic vector and scalar potential using NU function analysis and its application for optical properties. The final keynote was provided to talk regarding superconductivity: first invention to current application. While for the conference participants, there is 303 participant which was submitted abstract via the conference system. Then, the 186 full papers have been submitted from the participant, and after the reviewed process, 136 papers have been presented in the ICSAS 2021. And then for the final decision, 116 papers published in AIP Conference Proceedings.

We would like to thank all of the participants attending this conference and also to the committee for their contribution to this high-level conference and its overall success. We also would like to thank the reviewers for their positive contribution to maintain the quality of the articles presented at this conference.

Editorial Boards
Budi Purnama (Editor in Chief)
Dewanta Arya Nugraha
A Suparmi

Committees

Advisory Board

1. Prof. A. Rusydi, Physics Department, National University Singapore,
2. Prof. S. Yoshimura, Akita University, Japan.
3. Dr. Isao Watanabe, RIKEN Nishina Center, Wako, Saitama, Japan
4. Ari Handono Ramelan, Universitas Sebelas Maret, Indonesia
5. Cari, Universitas Sebelas Maret, Indonesia
6. Harjana, Universitas Sebelas Maret, Indonesia
7. Suparmi, Universitas Sebelas Maret, Indonesia

Chairman

Budi Purnama, Universitas Sebelas Maret, Indonesia

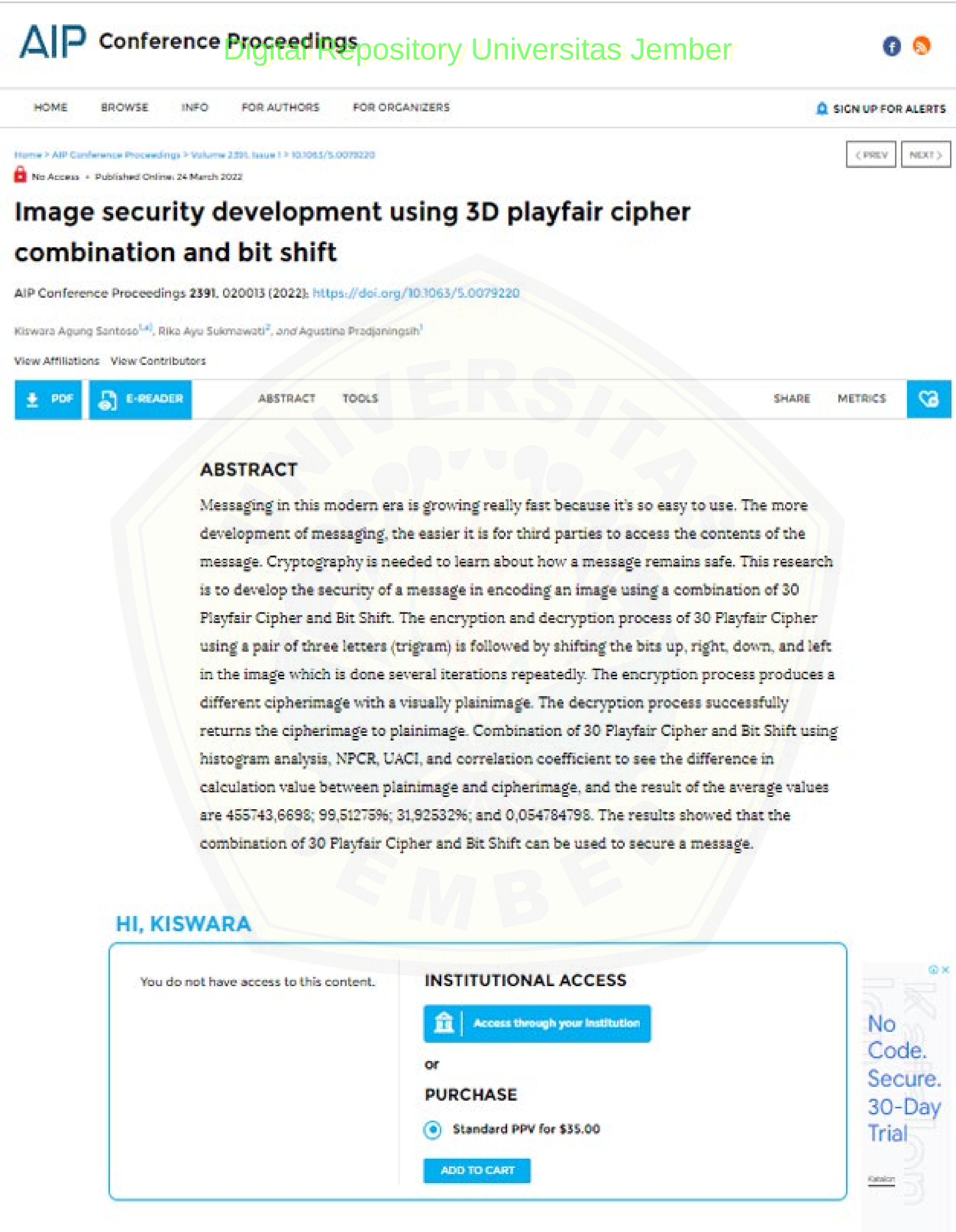
Organizing Committee

1. Agus Supriyanto, Universitas Sebelas Maret, Indonesia
2. Ahmad Marzuki, Universitas Sebelas Maret, Indonesia
3. Artono Dwijo Sutomo, Universitas Sebelas Maret, Indonesia
4. Budi Legowo, Universitas Sebelas Maret, Indonesia
5. Dewanta Arya Nugraha, Universitas Sebelas Maret, Indonesia
6. Fahru Nurosyid, Universitas Sebelas Maret, Indonesia
7. Fuad Anwar, Universitas Sebelas Maret, Indonesia
8. Hendri Widyandari, Universitas Sebelas Maret, Indonesia
9. Iwan Yahya, Universitas Sebelas Maret, Indonesia
10. Khairuddin, Universitas Sebelas Maret, Indonesia
11. Kusumandari, Universitas Sebelas Maret, Indonesia
12. Mohtar Yunianto, Universitas Sebelas Maret, Indonesia
13. Nuryani, Universitas Sebelas Maret, Indonesia
14. Risa Suryana, Universitas Sebelas Maret, Indonesia
15. Utari, Universitas Sebelas Maret, Indonesia
16. Yofentina Iriani, Universitas Sebelas Maret, Indonesia

Organizer

UNS
UNIVERSITAS
SEBELAS MARET

Physics Department,
Faculty of Mathematics and Natural Sciences,
Universitas Sebelas Maret, Indonesia


AIP Conference Proceedings
HOME
BROWSE
INFO
FOR AUTHORS
FOR ORGANIZERS
SIGN UP FOR ALERTS
Home > AIP Conference Proceedings > Volume 2391, Issue 1 > 10.1063/5.0079220
‹ PREV
NEXT ›

No Access • Published Online: 24 March 2022

Image security development using 3D playfair cipher combination and bit shift

AIP Conference Proceedings **2391**, 020013 (2022); https://doi.org/10.1063/5.0079220

Kiswara Agung Santoso[1,a)], Rika Ayu Sukmawati[2], and Agustina Pradjaningsih[1]

ABSTRACT

Messaging in this modern era is growing really fast because it's so easy to use. The more development of messaging, the easier it is for third parties to access the contents of the message. Cryptography is needed to learn about how a message remains safe. This research is to develop the security of a message in encoding an image using a combination of 3D Playfair Cipher and Bit Shift. The encryption and decryption process of 3D Playfair Cipher using a pair of three letters (trigram) is followed by shifting the bits up, right, down, and left in the image which is done several iterations repeatedly. The encryption process produces a different cipherimage with a visually plainimage. The decryption process successfully returns the cipherimage to plainimage. Combination of 3D Playfair Cipher and Bit Shift using histogram analysis, NPCR, UACI, and correlation coefficient to see the difference in calculation value between plainimage and cipherimage, and the result of the average values are 455743,6698; 99,51275%; 31,92532%; and 0,054784798. The results showed that the combination of 3D Playfair Cipher and Bit Shift can be used to secure a message.

HI, KISWARA

You do not have access to this content.

INSTITUTIONAL ACCESS

or

PURCHASE

● Standard PPV for $35.00

Image Security Development Using 3D Playfair Cipher Combination and Bit Shift

Kiswara Agung Santoso[1,a)], Rika Ayu Sukmawati[2,b)], Agustina Pradjaningsih[1,c)]

[1] *University of Jember*
Jl. Kalimantan No. 37 KampusTegal Boto,Jember, Indonesia

[2] *Master Program of Mathematics Department, Faculty of Science, University of Jember*
Jl. Kalimantan No. 37 KampusTegal Boto,Jember, Indonesia

[a)]Corresponding author: kiswara.fmipa@unej.ac.id

Abstract. Messaging in this modern era is growing really fast because it's so easy to use. The more development of messaging, the easier it is for third parties to access the contents of the message. Cryptography is needed to learn about how a message remains safe. This research is to develop the security of a message in encoding an image using a combination of 3D Playfair Cipher and Bit Shift. The encryption and decryption process of 3D Playfair Cipher using a pair of three letters (trigram) is followed by shifting the bits up, right, down, and left in the image which is done several iterations repeatedly. The encryption process produces a different cipherimage with a visually plainimage. The decryption process successfully returns the cipherimage to plainimage. Combination of 3D Playfair Cipher and Bit Shift using histogram analysis, NPCR, UACI, and correlation coefficient to see the difference in calculation value between plainimage and cipherimage, and the result of the average values are 455743,6698; 99,51275%; 31,92532%; and 0,054784798. The results showed that the combination of 3D Playfair Cipher and Bit Shift can be used to secure a message.

INTRODUCTION

The development of increasingly sophisticated technology makes it easier for a person to send a message to another person, but this can also make third parties to access or sabotage the contents of the message, so a science called cryptography is needed to secure the message content. Cryptography is science for protecting or hiding messages from being discovered by third parties by changing the original message content into codes that are difficult to understand. There are several methods used in cryptography, including the 3D Playfair Cipher. 3D Playfair Cipher is a cryptographic method whose encryption and decryption process uses a key that will be written on four 4 × 4 tables that support 10 digit numbers (0-9), 26 letters (AZ), and 28 special characters which will then be used reference for the encryption and decryption process. 3D Playfair Cipher works in trigram form as an encryption and decryption process [1].

This research, it discusses the increased security of image encoding using a combination of 3D Playfair Cipher and Bit Shift, which encryption results are analyzed using histogram analysis, NPCR, UACI, and correlation coefficients.

Cryptography

Cryptography is a science in the field of computational mathematics that studies how a message or information remains safe and cannot be known by unauthorized parties. There are several aspects that must be fulfilled in information security, namely aspects of confidentiality, data integrity, authentication and non-repudiation..

Cryptography (cryptography) is the science and art of keeping messages to safe. Crypto means secret and graphy means writing . Cryptography can be interpreted as writing or secret messages. The secret message is called plaintext, while the encrypted message is called ciphertext. The process of encoding plaintext into ciphertext is called encryption and the process of reversing ciphertext into plaintext is called decryption [2].

3D Playfair Cipher

3D Playfair Cipher is a cryptographic method that uses four 4 × 4 tables to write a key as a reference for completing the encryption and decryption process.

TABLE 1. Keys at 3D Playfair Cipher

LEVEL 1					LEVEL 2			
0	1	2	3		G	H	I	J
4	5	6	7		K	L	M	N
8	9	A	B		O	P	Q	R
C	D	E	F		S	T	U	V

LEVEL 3					LEVEL 4			
W	X	Y	Z		-	.	/	:
!	“	=	$		;	<	=	>
%	&	‘	(		?	@	[	\
)	*	+	,		]	^	_	|

The encryption process in 3D Playfair Cipher is that the plaintext will be broken down into trigrams (pairs of three letters). The extra letters X and Z are used to fill the trigraph, X is added when there is one blank space left in the message, X and Z are added when there are two blank spaces. For example LOLLIPOP will be changed to {LOL}, {LIP}, {OPX}, and GOODGRACES to be {GOO}, {DGR}, {ACE), {SXZ). The encryption and decryption process uses a circular model, where the replacement of letters in a trigram will be replaced by messages related to the position of letters in trigrams in rows, columns, and levels in a circular manner [1].

TABLE 2. Encryption process in 3D Playfair Cipher

Trigram	**Trigram Plaintext**			**Trigram**
Plaintext	**Char-1**	**Char-2**	**Char-3**	**Ciphertext**
Char-1	Row	Column	Level	**Char-1**
Char-2	Level	Row	Column	**Char-2**
Char-3	Column	Level	Row	**Char-3**

The decryption process is the same as the encryption process, namely with a circular model, but only differs in the order, namely rows, levels, columns in the trig [1].

TABLE 3. Decryption process on the 3D Playfair Cipher

Trigram	**Trigram Ciphertext**			**Trigram**
Ciphertext	**Char-1**	**Char-2**	**Char-3**	**Plaintext**
Char-1	Row	Level	Column	**Char-1**
Char-2	Column	Row	Level	**Char-2**
Char-3	Level	Column	Row	**Char-3**

Base of Number

The number based on its basis consists of several kinds including decimal and binary numbers. A decimal number is a number that has a base of 10, namely 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Binary numbers are numbers that have bases of 2, namely 0 and 1. a number base can be converted to another base number, namely from decimal to binary and from binary to decimal [3].

Binary numbers have several number operations, one of which is XOR. p and q are a proposition. The false statement is stated in bit 0 and the correct statement is stated in bit 1 as in TABLE 4.

TABLE 4. Binary XOR operations

P	***Q***	***p* ⊕ *q***
1	1	0
1	0	1
0	1	1
0	0	0

Bit Shift

The bit shift used is a 1-bit leftward shift. In the shift, there is a rule that is if the leftmost bit before being shifted is 1 then it will be XORed with 0001 1011 whereas if the leftmost bit is 0 before the shift occurs then there is no need to XOR with 0001 1011 and after the shift, the right end bit written as 0 [3].

Image

Image is an image on a two-dimensional plane. image can be computed in a computer program if the image is digitized first. Image has two types, namely grayscale image and RGB image (color image).

A grayscale image is a digital image that only has one channel value per pixel, meaning that the value of Red = Green = Blue. These values are used to indicate color intensity. The displayed image consists of gray color, varies in black as the weakest intensity and white as the strongest intensity [4].

The color of the image is an image whose pixel value represents a certain color. The number of colors that may be used depends on the pixel depth of the image in question. RGB images are represented in several channels which represent the constituent color components. The number of channels used depends on the color model used in the image [5].

ASCII

ASCII (American Standard Code for Information Intercange) is an international standard in code letters and symbols that is universal. ASCII is used by computers and other communication tools to show text [5].

ASCII is a code used to represent letters, numbers and symbols. The number of ASCII number is 250 codes. ASCII 0-127 is the code for text manipulation, while ASCII 128-255 is the code for graphic manipulation.

Histogram Analysis

The histogram analysis technique was used to see the suitability of the color distribution between plainimage and cipherimage. If the cipherimage histogram has a variety of distributions and has a significant difference with the plainimage, it can be said that the cipherimage does not provide a clue to perform a statistical attack on the resulting cipherimage. The X^2 test was used to analyze the histogram uniformity of the encrypted image.

$$X^2 = \sum_{i=0}^{255} \frac{(v_i - v_0)^2}{v_0} \tag{1}$$

where v_i is the observed frequency of the pixel value $i (0 \leq i \leq 255)$ and v_0 is the expected frequency of a pixel *i* value, so $v_0 = \frac{m \times n}{256}$, where m is the image length and n is the image width . The smaller the result of X^2, the uniformity level in the histogram is more evenly distributed and the results of the encryption are better (safe), while the greater the result of X^2, the level of uniformity in the histogram will be more uneven and the results of the encryption are certainly not good (not safe) [6].

NPCR

NPCR (Number of Pixel Change Rate) is to guarantee that each pixel has a change in the color element.

$$NPCR = \left(\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{o}\frac{d_{i,j,k}}{T}\right) \times 100\% \qquad (2)$$

The value of *d*(*i,j,k*) is the number of pixel differences multiplied by the value 100% then divided by the width and height of the sample image. Channels in each type of image are different, including Greyscale which has 1 channel, black and white has 2 channels, and RGB has 3 channels. Cipherimage can be said to be good (safe) if the value on the NPCR indicator is greater [6].

UACI

UACI (Unified Averaged Changed Intensity) is one of the parameters used to analyze changes in one pixel in plainimage which causes major changes in cipherimage.

$$UACI = \left(\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{o}\frac{|C_1(i,j,k) - C_2(i,j,k)|}{F.T}\right) \times 100\% \qquad (3)$$

Cipherimage can be said to be good (safe) if the value on the UACI indicator is greater [6].

Correlation Coefficient

The correlation coefficient is used to measure the relationship between two variables, namely plainimage and cipherimage. The algorithm used can be said to be safe if the cipherimage is completely different from the plainimage.

$$CorrCoef\,(\mathrm{x,y}) = \frac{\sum_{i=1}^{n}(x_i - \mu(x))(y_i - (\mu(y))}{\sigma(x)\sigma(y)} \qquad (4)$$

where $\mu(x)$ and $\mu(y)$ are the mean of *x* and *y* respectively obtained from equation (5).

$$\mu(x) = \frac{1}{n}\sum_{i=1}^{n} x_i \text{ and } \mu(y) = \frac{1}{n}\sum_{i=1}^{n} y_i \qquad (5)$$

x and *y* are variables of plainimage and cipherimage.

Standard deviation (σ) is used to find out how close the distribution of data is to the average value. Here is equation (6) about the standard deviation for *x* and *y*, respectively.

$$\sigma(x) = \sqrt{\sum_{i=1}^{n}(x_i - \mu(x))^2} \text{ and } \sigma(y) = \sqrt{\sum_{i=1}^{n}(y_i - \mu(y))^2} \qquad (6)$$

If the correlation coefficient is equal to one, then the plainimage and cipherimage are identical. If the coefficient is equal to zero, then plainimage is different from cipherimage and it can be said that encryption is good [7].

METHODOLOGY

The data used for testing in this study were 2 keys and 10 images. The research steps carried out are as follows:

1. Literature Study
   Literature studies are carried out by studying references related to cryptography, 3D Playfair Cipher, Bit Shift, Image, ASCII, and also studying security analysis including histogram analysis, NPCR, UACI, and correlation coefficients.
2. Research Process
   This research process is to perform encryption and decryption process on an image using a combination of 3D Playfair Cipher and Bit Shift. Encryption and decryption are processed using the 3D Playfair Cipher first, then proceed using Bit Shift, namely shifting bits up, right, down, and left. The process is carried out in a predetermined number of iterations.
3. Development Program and Simulation Program

Making encryption and decryption programs using a combination of 3D Playfair Cipher on images using MATLAB R2015b software and simulated existing data in the program.

4. Results Safety Analysis
The safety analysis of the results was carried out by comparing the calculation results of the histogram analysis, NPCR, UACI, and the correlation coefficient. So it can be analyzed the comparison of image security before and after encryption using a combination of 3D Playfair Cipher and Bit Shift.

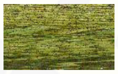
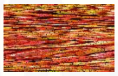
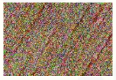
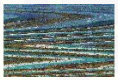
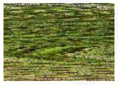
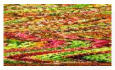
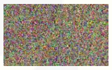
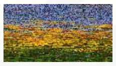
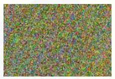
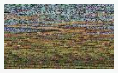
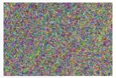
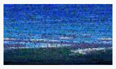
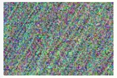
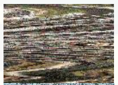
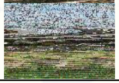
RESULTS AND DISCUSSION

Results

The simulation is carried out by encrypting 10 images with 2 different keys.

1. The result of the encryption process uses a combination of 3D Playfair Cipher and Bit Shift.

TABLE 5. Results of the encryption process

No	Research Data	Key	3D Playfair Cipher	3D Playfair Cipher and Bit Shift
1		bitshift		
2		playfaircipher		
3		bitshift		
4		playfaircipher		
5		bitshift		
6		playfaircipher		
7		bitshift		
8		playfaircipher		
9		bitshift		
10		playfaircipher		

2. The Results of the X^2 calculation use a Combination of 3D Playfair Cipher and Bit Shift.

TABLE 6. Calculation results X^2

No	Research Data	Key	X^2	
			3D Playfair Cipher	**3D Playfair Cipher and Bit Shift**
1	Image 1	bitshift	1633386,7446	86031,5347
2	Image 2	playfaircipher	14381372,3394	2116627,1637
3	Image 3	bitshift	1273781,7323	21256,7076
4	Image 4	playfaircipher	1589577,9628	157509,8118
5	Image 5	bitshift	3844672,6758	387086,1335
6	Image 6	playfaircipher	20465287,0386	2247977,5608
7	Image 7	bitshift	4349398,2781	25531,2186
8	Image 8	playfaircipher	8708443,8787	198766,9683
9	Image 9	bitshift	685550,3418	33977,9038
10	Image 10	playfaircipher	634298,5046	40134,1043

3. The NPCR results use a combination of 3D Playfair Cipher and Bit Shift.

TABLE 7. NPCR results

No	Research Data	Key	3D Playfair Cipher	3D Playfair Cipher and Bit Shift
1	Image 1	bitshift	88,57%	99,58%
2	Image 2	playfaircipher	82,67%	99,22%
3	Image 3	bitshift	92,06%	99,60%
4	Image 4	playfaircipher	88,47%	99,48%
5	Image 5	bitshift	84,55%	99,47%
6	Image 6	playfaircipher	88,70%	99,24%
7	Image 7	bitshift	92,10%	99,61%
8	Image 8	playfaircipher	87,35%	99,59%
9	Image 9	bitshift	90,31%	99,60%
10	Image 10	playfaircipher	90,90%	99,60%

4. UACI results use a combination of 3D Playfair Cipher and Bit Shift.

TABLE 8. UACI results

No	Research Data	Key	3D Playfair Cipher	3D Playfair Cipher and Bit Shift
1	Image 1	bitshift	10,35%	29,55%
2	Image 2	playfaircipher	7,60%	33,40%
3	Image 3	bitshift	10,10%	30,30%
4	Image 4	playfaircipher	9,13%	30,39%
5	Image 5	bitshift	6,54%	33,78%
6	Image 6	playfaircipher	17,66%	32,13%

No	Research Data	Key	3D Playfair Cipher	3D Playfair Cipher and Bit Shift
7	Image 7	bitshift	17,76%	30,11%
8	Image 8	playfaircipher	12,12%	33,89%
9	Image 9	bitshift	8,08%	31,25%
10	Image 10	playfaircipher	16,42%	34,41%

5. The results of the correlation coefficient use a combination of 3D Playfair Cipher and Bit Shift.

TABLE 9. Correlation Coefficient Results

No	Research Data	Key	3D Playfair Cipher	3D Playfair Cipher and Bit Shift
1	Image 1	bitshift	0,6457	0,0527
2	Image 2	playfaircipher	0,8469	0,1854
3	Image 3	bitshift	0,6852	0,0004
4	Image 4	playfaircipher	0,6968	0,0783
5	Image 5	bitshift	0,9005	0,0973
6	Image 6	playfaircipher	0,4966	0,0924
7	Image 7	bitshift	0,2593	0,0067
8	Image 8	playfaircipher	0,6452	0,0375
9	Image 9	bitshift	0,8117	0,0072
10	Image 10	playfaircipher	0,5075	-0,0068

Discussion

The results showed that the image encryption process using a combination of 3D Playfair Cipher and Bit Shift looks random (no pattern) so it is difficult to predict the original image. The image encryption process using a combination of 3D Playfair Cipher and Bit Shift is also implemented through the MATLAB R2015b program based on the method proposed by the author.

The decryption process is the opposite of the encryption process. The results obtained from the decryption process using a combination of 3D Playfair Cipher and Bit Shift can restore the cipherimage to a plainimage image. The image decryption process using a combination of 3D Playfair Cipher and Bit Shift is also implemented through the MATLAB R2015b program based on the method proposed by the author.

The results of the histogram analysis in this study show that the combination of 3D Playfair Cipher and Bit Shift produces a more evenly histogram with a smaller X^2 calculation than the histogram results using 3D Playfair Cipher which can be seen in Table 6. Meanly, the results of the encryption process using The combination of 3D Playfair Cipher and Bit Shift will be safer and stronger against attacks than using 3D Playfair Cipher.

The results of the NPCR calculation in this study show that the combination of 3D Playfair Cipher and Bit Shift produces a greater NPCR value than the results of the NPCR value using 3D Playfair Cipher which can be seen in Table 7. The results of UACI calculations in this study show that the combination of 3D Playfair Cipher and Bit Shift produces The UACI value is greater than the UACI value using the 3D Playfair Cipher which can be seen in Table 8. While the results of the calculation of the correlation coefficient in the study show that the combination of the 3D Playfair Cipher and Bit Shift produces a correlation coefficient value that is greater than the 3D Playfair Cipher which can be seen in Table 9. Based on the results that have been obtained, the greater the results of the calculation of the NPCR, UACI, and the correlation coefficient, the stronger the encrypted image is against the attack.

CONCLUSIONS

Based on the results of the research that has been done, the following conclusions are obtained:

1. The encryption process using a combination of 3D Playfair Cipher and Bit Shift is successful because it is clear that plainimage and cipherimage are very different visually. Likewise, the decryption process using a combination of 3D Playfair Cipher and Bit Shift was successful because the cipherimage was back to its original plainimage.
2. The results of the comparison of the security level of encrypted images using 3D Playfair Cipher with a combination of 3D Playfair Cipher and Bit Shift based on histogram analysis, NPCR, UACI, and correlation coefficients are as follows:
   - Based on the results of histogram analysis, the level of security of encrypted images using a combination of 3D Playfair Cipher and Bit Shift is safer than 3D Playfair Cipher, this is because the calculation of the X^2 value combination of 3D Playfair Cipher and Bit Shift is smaller than 3D Playfair Cipher and 3D combination histogram graph. Playfair Cipher and Bit Shift are more evenly distributed than 3D Playfair Cipher because no pixels dominate.
   - Based on the NPCR results, the security level of encrypted images using a combination of 3D Playfair Cipher and Bit Shift is safer than 3D Playfair Cipher, this is because the NPCR value of the combination of 3D Playfair Cipher and Bit Shift is greater than 3D Playfair Cipher.
   - Based on the UACI results, the security level of encrypted images using a combination of 3D Playfair Cipher and Bit Shift is safer than 3D Playfair Cipher, this is because the UACI value of the combination of 3D Playfair Cipher and Bit Shift is greater than 3D Playfair Cipher.
   - Based on the correlation coefficient results, the security level of encrypted images using a combination of 3D Playfair Cipher and Bit Shift is safer than 3D Playfair Cipher, this is because the UACI value of the combination of 3D Playfair Cipher and Bit Shift is greater than 3D Playfair Cipher.

REFERENCES

[1] Singh.S, R.Jain, and P.Deep.Agarwal, Developing Mobile Message Security Application Using 3D Playfair Cipher Algorithm, ICACEA, (2015), pp. 838-841.

[2] Santi.R.C.N, Implementasi Algoritma Enkripsi Playfair pada File Teks, *Jurnal Teknologi Informasi DINAMIK*. (2010), pp. 15(1) 27-33

[3] Riski, A, A.S Rizal and A. Kamsyakawuni, Pengamanan Citra dengan Operator Algoritma Genetika, (2019), Vol. 4 No. 1

[4] Sholehah.D.P.T, Penerapan Algoritma DNA-Vigenere Cipher dengan Kunci Citra Grayscale pada Data Teks, *Skripsi*, Jember: Universitas Jember. (2017)

[5] Muhendra.A.Z, Implementasi Kriptografi Affine Cipher pada Citra Digital Hasil Steganografi Metode Parity Coding dengan Pseudo Random Number Generator (PRNG), *Skripsi*, Jember: Universitas Jember. (2016)

[6] Boriga.R.E, A.C.Dăscălescu, and A.V.Diaconu, A New Fast Image Encryption Scheme Based on 2D Chaotic Maps, *IAENG International Journal of Compuer Science* 41 (4). (2014)

[7] Mousa, A., O. S. F. Allah., and E. S. M. Nigm, Security Analysis of Reverse Encryption Algorithm for Databases, International Journal of Computer Applications *(0975 – 8887)*, (2013) pp. 66(14):19-27.