Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 8, No. 2, May, Pp. 535-544

Visual analysis based on CMY and RGB image cryptography using vigenere and beaufort cipher

Christy Atika Sari*[1], Danang Wahyu Utomo[2], Mohamed A S Doheir[2]
Informatics Engineering, Computer Science Faculty, Universitas Dian Nuswantoro, Indonesia[1]
Computer Engineering, University Malaysia of Computer and Engineering, Malaysia[2]

Article Info
Keywords:
Vigenere Cipher, Beaufort Cipher, Fibonacci, Color Image, Cryptography

Article history:
Received: January 12, 2023
Accepted: March 08, 2023
Published: May 31, 2023

Cite:
C.Atika Sari, D. W. Utomo, and M. A. S. Doheir, "Visual Analysis Based on CMY and RGB Image Cryptography Using Vigenere and Beaufort Cipher", KINETIK, vol. 8, no. 2, May 2023.
https://doi.org/10.22219/kinetik.v8i2.1664

*Corresponding author.
Christy Atika Sari
E-mail address:
christy.atika.sari@dsn.dinus.ac.id

Abstract
The achievement of visual aspects and image security often cannot meet visibility standards, for example the acquisition of PSNR and UACI NPCR values. To increase security, this research has implemented a combination of the Vigenere cipher and Beaufort and the use of Fibonacci as a randomizer. The combination of the Vigenere Cipher and Beaufort Cipher substitution algorithms with the Fibonacci technique can be applied to encrypt color images in RGB and CMY, with a size of 256x256 pixels and in .bmp format. The Fibonacci cut-off value used in this study is 10000. The highest entropy value of the cipher image peppers.bmp is 7,991. The lowest PSNR cipher image value is accordion.bmp where for RGB it is 5,439 dB and for CMY it is 5,403 dB. accordion.bmp's highest UACI value is 44.018% for RGB and 44.312% for CMY. The NPCR value in the airplane.bmp image has the highest value in RGB of 99.792% and for CMY the highest value is in splash.bmp with a value of 99.798%. Evaluation of the decryption results shows that the decryption process can run perfectly as indicated by the values of MSE=0, PSNR=inf, UACI and NPCR=0%. Therefore, encrypt and decrypt was proven that the results obtained in the visual aspect are very good.

1. Introduction

In this technological era, where connectedness via the Internet continues to increase, the importance of data security is also increasing. Data security is the practice of protecting digital information from access by unauthorized persons, data damage or data theft during its existence on the Internet. This includes digital and physical security, which means hardware such as storage devices that are used to store data [1]–[3], as well as software that takes care of security in the form of program logic or algorithms. Cryptography [4] has been developed to encrypt and decrypt user data, to maintain the security of their activities on the Internet and prevent various criminal acts. In this paper, the encryption and decryption methods that will be discussed are cryptographic methods that use sequences of Fibonacci numbers. Cryptography is essentially encoded writing, which has been used to exchange confidential information since 1900 BC, documented in the use of non-standard hieroglyphs in inscriptions [5]–[7]. Since then, many other uses of cryptography have appeared, scattered in various times and places. Because its function is to hide secret messages, of course, it takes many ways to convert these messages into code. Therefore, there are many methods of converting a message into a code (encryption) and converting the code back into a message that can be read by the recipient (decryption).

Vigenere Cipher [8] is included in the type of substitution cipher and is included in the symmetric key algorithm, which uses the same key for the encryption and decryption process. The Vigenere Cipher encryption process converts plaintext into ciphertext based on the key used. The key used in this algorithm must be the same length as the plaintext. There are two ways of encrypting and decrypting the Vigenere Cipher, the first is using the tabula recta table, the second is using the modulo 26 function. Beaufort Cipher is a derivative of the Vigenere Cipher algorithm. Beaufort Cipher and Vigenere Cipher are both included in substitution cryptography with symmetric keys. The Beaufort Cipher has a slight difference from the Vigenere Cipher which lies in the formula that will be used in the encryption and decryption process. In the Beaufort Cipher [9], to perform encryption and decryption by subtracting the key used with the plaintext or ciphertext.The Fibonacci [10] sequence is a series that starts from the first 2 numbers, then the next number is obtained by adding the two previous numbers. This Fibonacci sequence starts with the numbers 0 and 1. Examples of the Fibonacci sequence are 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, and so on. In this research, an analysis has been carried out on the results of encryption and decryption using Fibonacci on the vigenere-beaufort and beaufort-vigenere schemes.

2. Research Method

2.1 State of The Art

Super encryption uses a Column Transposition algorithm based on the Vigenere Cipher on images [11]. In this study, the digital image is encrypted using Column Transposition first, then the encrypted image is encrypted again using the Vigenere Cipher. This combination of Column Transposition and Vigenere Cipher can work well in various image sizes. The time to encrypt images is relatively longer than the time to decrypt images. The PSNR value of the original image and the decrypted image is inf, which means that the original image and the decrypted image have not changed at all, and the measurement results of the SSIM method show the number 1 which proves that the image decryption process is running perfectly. Modification of the Vigenere Cipher algorithm for digital image encryption [12]. The encryption process and the digital image decryption process by randomizing the image pixel values using the Vigenere Cipher where the key is modified with a Linear Congruent Generator random number generator. The tests carried out resulted in an increase in entropy values for all encrypted images. So that the modification of the Vigenere Cipher algorithm and the Linear Congruent Generator are strong enough to encrypt images. The key used is a series of numbers so that the Kasiski method cannot find the length of the key used Digital image encryption uses a combination of Beaufort Cipher and Vigenere Cipher [13]. The encryption and decryption process in this study uses 2 random keys. The results of this study were measured using PSNR and MSE by comparing PSNR and MSE cipher image values using a combination of Beaufort Cipher and Vigenere Cipher, with the Beaufort Cipher algorithm only or the Vigenere Cipher only. PSNR and MSE cipher image values with a combination of these two algorithms are superior to using only one algorithm. Evaluation of the PSNR value of the decrypted image and the original image is inf, ie the decrypted image and the original image are exactly the same. Meanwhile, the MSE value of the decrypted image and the original image is 0, which means that there is no change in the pixel value between the original image and the decrypted image. Making applications with One Time Pad Cipher and Affine Cipher and Fibonacci algorithms as in [14]. Fibonacci in this study is used to form keys based on plaintext that will be used in One Time Pad Cipher. This study concludes that Fibonacci can be used to create keys so that there are no repeated characters in the key. Several study has illustrated in Table 1, where VC = Vigenere Cipher, CC = Chaos Cipher, BC = Beaufort Cipher, OTP = One Time Pad, AC = Affine Cipher, CT = Columnar Transposition, LCG = Linear Congruential Generator.

Table 1. State of The Art

Author	Year	Methods					Optimation		Results
		VC	BC	OTP	AC	CT	LCG	Fibonacci	
Sinaga, et. al. [11]	2018	✓				✓			The fastest time for encryption is 0.100510 seconds, and the longest time is 10.148356 seconds. The highest PSNR value from the decrypted image is inf, and the SSIM measurement result is 1.
Marsal, et. al. [12]	2018	✓					✓		The difference in cipherimage entropy values with the initial image produces the largest difference is 6.540333 and the smallest difference is 0.431984.
Setiadi, et. al. [13]	2018	✓	✓						The PSNR value of the highest cipherimage is 9.6277 dB with an MSE value of 7084.4516. The PSNR value of the decrypted image is inf and the MSE value is 0.
Firdaus, et. al. [14]	2017			✓	✓			✓	The Fibonacci sequence can be used to form keys in the One Time Pad Cipher based on the plaintext so that the resulting key does not contain repeated characters.

2.2. Vigenere Cipher

Vigenere Cipher is included in the type of substitution cipher and is included in the symmetric key algorithm, which uses the same key for the encryption and decryption process. The Vigenere Cipher encryption process converts plaintext into ciphertext based on the key used. The key used in this algorithm must be the same length as the plaintext. There are two ways to encrypt and decrypt the Vigenere Cipher, the first is using the tabula recta table, the second is using the modulo 26 functions [15]–[17]. Here's an example of the tabula recta for the Vigenere Cipher as shown in Figure 1. Encryption uses tabula recta by drawing a line from the plaintext downwards (vertically), and dragging a line from the key to the right (horizontally). Of the two lines there is an intersection, the letter at the intersection is the ciphertext. Meanwhile, to decrypt is the opposite, namely by drawing a line from the key horizontally to the right up to the ciphertext, then draw a line up towards the plaintext using tabula recta as shown in Table 2.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 1. Tabula Recta Vigenere

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 2. Example of Vigenere Cipher Encryption with Tabula Recta

Plaintext: MICHELLE, and Key: UDINUS. The way the Vigenere Cipher works is by repeating the key up to the length of the plaintext, so that it becomes: Plaintext is MICHELLE, Key is UDINUSUD, and Ciphertext is GLKUYDFH. Threrefore, for plaintext the letter "M" and the key letter "U" produce the ciphertext letter "G" as shown in Figure 2. Do it like this until the plaintext is all encrypted. The mathematical formula for the Vigenere Cipher is in Equation 1, Where C= Ciphertext, P = Plaintext, K= Key.

$$C = (P + K) \bmod 26 \quad (1)$$

$$P = (C - K) \bmod 26 \quad (2)$$

An example of Vigenere Cipher encryption using Equation 1 and Equation 2, as shown below and Figure 3, using Plaintext : MICHELLE and Key: UDINUS. The key is repeated throughout the plaintext to become: Plaintext is MICHELLE and Key is UDINUSUD.

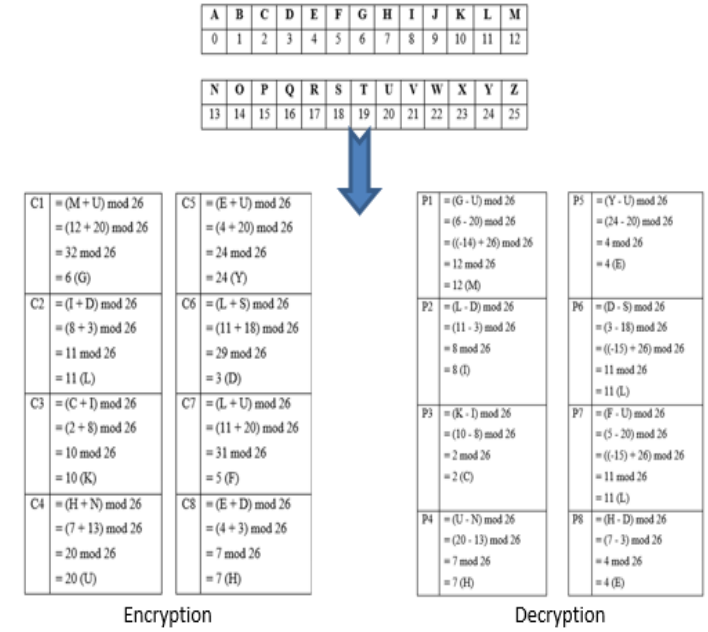


Figure 3. Example Calculation Using Vigenere Cipher

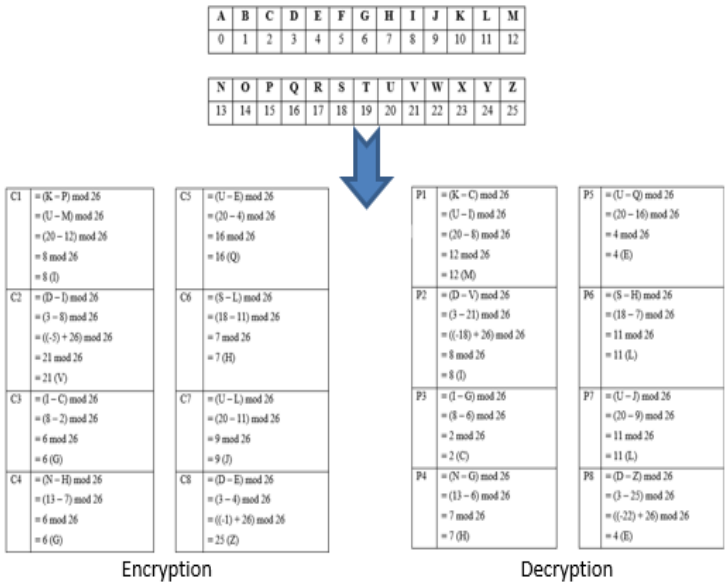


Figure 4. Example Calculation Using Beaufort Cipher

2.3 Beaufort Cipher

Beaufort Cipher is an algorithm derived from the Vigenere Cipher. Beaufort Cipher and Vigenere Cipher are both included in substitution cryptography with symmetric keys [9]. The Beaufort Cipher has a slight difference from the Vigenere Cipher which lies in the formula that will be used in the encryption and decryption process. In the Beaufort Cipher, to perform encryption and decryption by subtracting the key used with the plaintext or ciphertext as shown in Figure 5. Beaufort Cipher encryption and decryption using Equation 3 and Equation 4, where C= Ciphertext, P = Plaintext, K= Key. An example of encryption using the Beaufort Cipher using Plaintext : MICHELLE and Key: UDINUS. The key must be repeated all the way through the plaintext. Plaintext : MICHELLE and Key: UDINUSUD.

$$C = (K - P) \bmod 26 \quad (3)$$

$$P = (K - C) \bmod 26 \quad (4)$$

2.4 Proposed Method

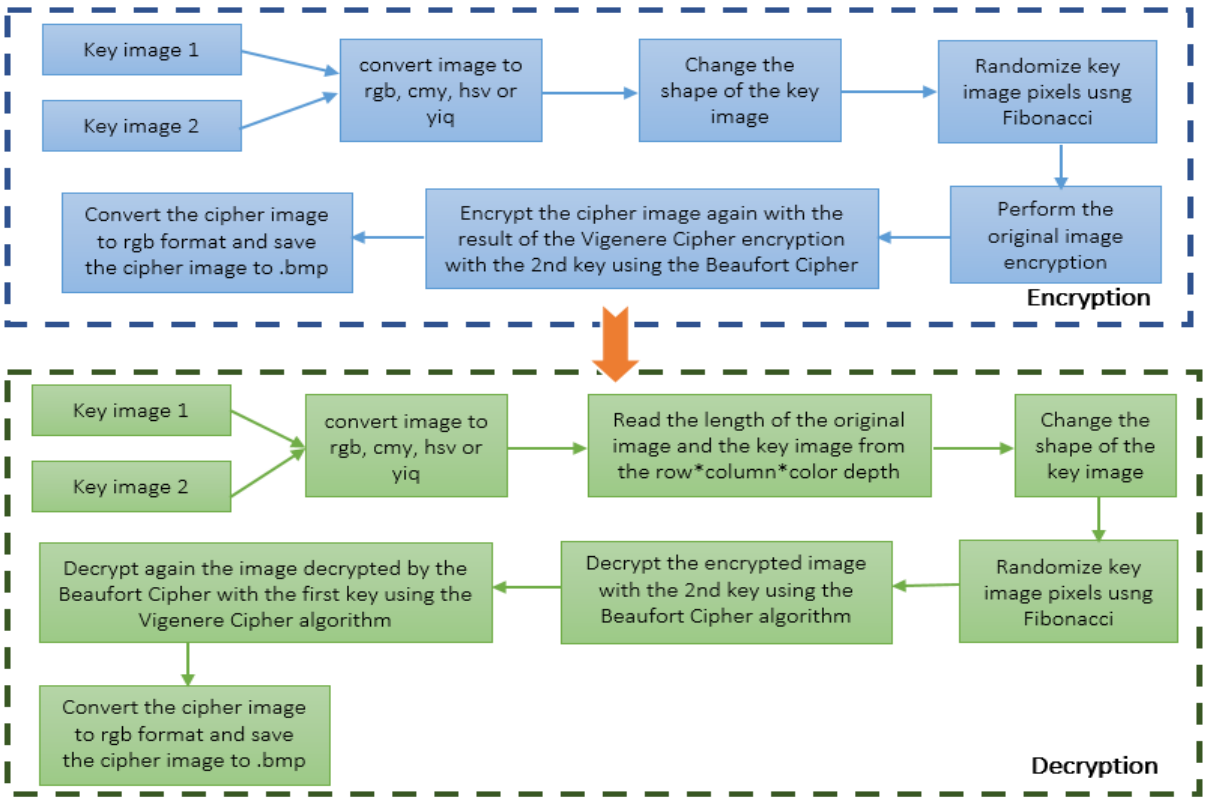


Figure 5. Encrypt and Decrypt Process

Image files are encrypted using the Vigenere Cipher and Beaufort Cipher algorithms as shown in Figure 5, which can be explained as follows:

1. Enter the original image, key image 1 and key image 2.
2. Convert the image to rgb, cmy, hsv or yiq format.
3. Read the length of the original image and the key image from the row*column*color depth.
4. Change the shape of the key image to a 1-dimensional array.
5. Randomize key image pixels using Fibonacci technique.
6. Perform the original image encryption process using key 1 with the Vigenere Cipher algorithm. Following Figure 6 is the pixel values from the original image which will be encrypted using the Vigenere Cipher. Encryption is done for each color component at each pixel up to the length of the image (row*column*color depth). If the image used is an RGB image with a size of 256 x 256 pixels, then the encryption process is repeated 256*256*3 = 196608 times. If the R value in the first pixel is 116 and the key in the first index is 139, then the Vigenere Cipher encryption result is ((116 + 139) mod 256) = 255. Therefore, 255 values are the result of the encryption of the R value in the first pixel. Figure 6 and Figure 7 shown the pixel value of the Vigenere Cipher image cipher.
7. Encrypt the cipher image again with the result of the Vigenere Cipher encryption with the 2nd key using the Beaufort Cipher algorithm. If the key at index 2 is 177 and the color value G in the first pixel is 239, then the cipher value is ((177 – 239) mod 256) = 194. Then the value of the cipher image G in the first pixel is 194.
8. Convert the cipher image to rgb format and save the cipher image to .bmp format as shown in Figure 8.

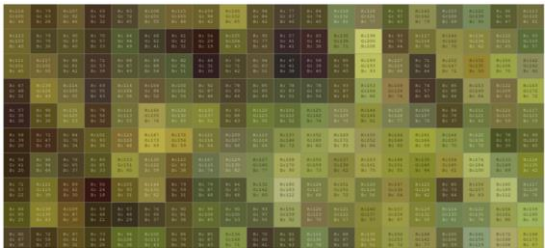


Figure 6. Original Image Pixel Value

Figure 7. Pixel Cipher Image Vigenere Cipher values

Figure 8. Pixel Cipher Image Beaufort Cipher values

The process of returning encrypted text files to their original form can be explained as follows:

1. Enter the cipher image and key images 1 and 2.
2. Change the cipher image, and key image into rgb, or cmycolor format.
3. Read the length of the image based on row*column*color depth.
4. Change the shape of the key image to a 1-dimensional array.
5. Randomize the key image pixels using Fibonacci.
6. Decrypt the encrypted image with the 2nd key using the Beaufort Cipher algorithm.
7. Decrypt again the image decrypted by the Beaufort Cipher with the first key using the Vigenere Cipher algorithm.
8. Change the decipher image to rgb format and save the decrypted image file in .bmp format.

3. Results and Discussion

Key images 1 and 2 will be transformed into 1-dimensional arrays. The results of these changes are shown in Figure 9 and Figure 10. Based Figure 9, the results of changing the key image to a 1-dimensional array, pixel values are randomized using Fibonacci. First, it takes as many Fibonacci numbers as the length of the image. If the image size is 256x256 pixels and in the RGB color space, then the required Fibonacci numbers are 256*256*3 = 196608 numbers. Then randomization is carried out based on the resulting numbers. Each Fibonacci number is performed modulo the image length, this aims to avoid Fibonacci numbers being larger than the image length. Each pixel value index that has appeared will be removed, and the length of the image will be reduced, this is done to avoid repeating pixel values. For example, it will take 6 pixel values from key image 1 which is already in the form of a 1-dimensional array as follow : 187 166 153 148 142 143. It takes 6 Fibonacci numbers, namely: 1 1 2 3 5 8. Randomize pixel values according to Fibonacci numbers as shown in Table 2.

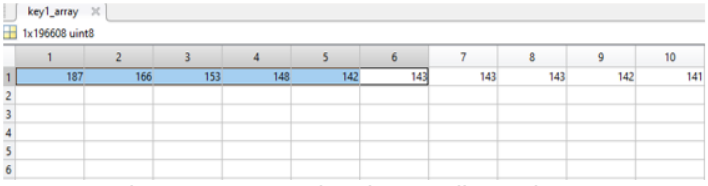


Figure 9. Array 1 key image dimensions 1

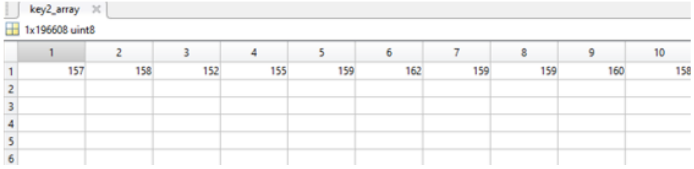


Figure 10. Array 1 key image dimensions 2

Table 2. Fibonacci Randomized

Loop	Pixel Value	Image length	Fibonacci (mod)	Random pixels
1st	187 166 153 148 142 143	6	1	187
2nd		5	1	166
3th		4	2	148
4th		3	0	143
5th		2	1	153
6th		1	0	142

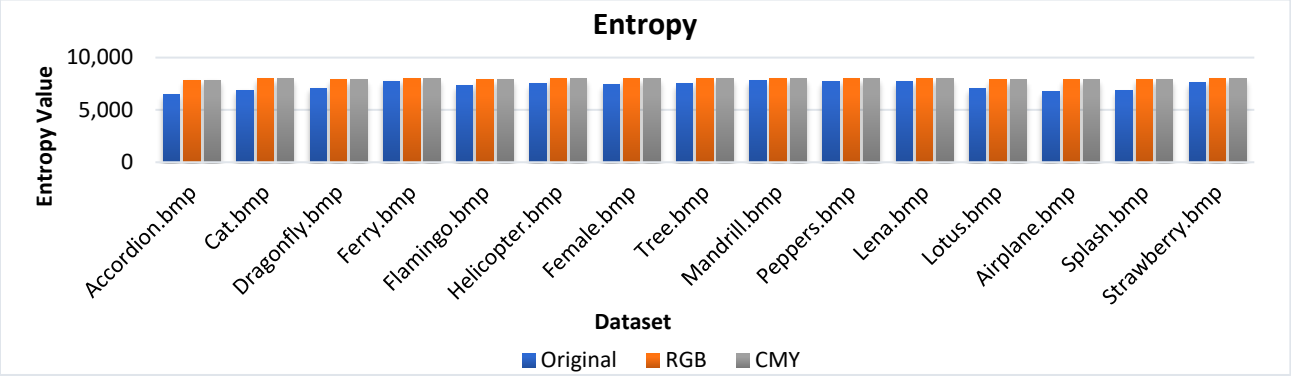


Figure 11. Entropy Cipher Image

The results of pixel values that have been randomized using Fibonacci is 187 166 148 143 153 142. After randomizing the pixels from key images 1 and 2, the encryption process is then carried out. The encryption process is done by calculating each image pixel value. Vigenere Cipher encryption of the original message image with a random key of 1 will produce a pixel value. From the resulting Vigenere cipher, the encryption process is carried out again with key 2 images whose pixel values have been randomized using the Beaufort Cipher algorithm. The entropy value of the Vigenere-Beaufort cipher image can be seen in Table 3. Based on Table 3, evaluating the entropy above, the resulting good cipher image has the highest entropy value of 7,991 in the peppers.bmp image. And all cipher images experience an increase in the entropy value of the original image. The results of the MSE and PSNR evaluation of the RGB and CMY cipher images are shown in Table 3. The results of the UACI and NPCR evaluations can be seen in Table 3

Table 3. MSE and PSNR Cipher Image Vigenere-Beaufort

Image Name	RGB		CMY		RGB		CMY	
	MSE	PSNR	MSE	PSNR	UACI (%)	NPCR (%)	UACI (%)	NPCR (%)
Accordion.bmp	18585.235	5.439	18741.430	5.403	44.018	99.597	44.312	99.595
Cat.bmp	12690.781	7.096	12792.087	7.061	36.622	99.632	36.867	99.669
Dragonfly.bmp	6523.538	9.986	6469.507	10.022	25.776	99.536	25.640	99.529
Ferry.bmp	13161.925	6.938	13170.652	6.935	37.512	99.662	37.512	99.664
Flamingo.bmp	10054.464	8.107	10036.573	8.115	32.866	99.666	32.817	99.675
Helicopter.bmp	14034.076	6.659	14032.384	6.659	39.387	99.706	39.333	99.704
Female.bmp	9183.106	8.501	9196.645	8.495	30.400	99.573	30.418	99.588
Tree.bmp	12942.660	7.011	12907.368	7.022	37.990	99.717	37.883	99.711
Mandrill.bmp	10334.755	7.988	10328.985	7.990	32.978	99.661	32.957	99.645
Peppers.bmp	12236.170	7.254	12225.196	7.258	36.196	99.685	36.205	99.687
Lena.bmp	10457.520	7.937	10420.233	7.952	33.056	99.634	32.957	99.636
Lotus.bmp	17249.761	5.763	17392.633	5.727	42.631	99.633	42.900	99.627
Airplane.bmp	13988.831	6.673	13877.728	6.708	40.079	99.792	39.832	99.789
Splash.bmp	11877.709	7.383	11953.652	7.356	36.980	99.783	37.137	99.798
Strawberry.bmp	15523.755	6.221	15607.164	6.198	39.499	99.573	39.637	99.533

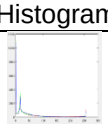
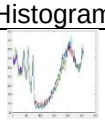
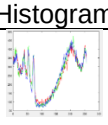
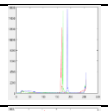
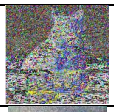
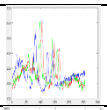
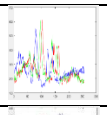
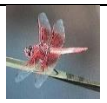
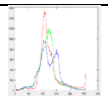
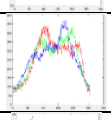
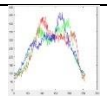
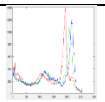
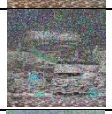
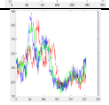
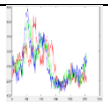
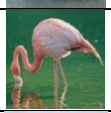
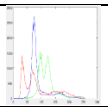
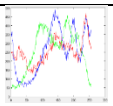
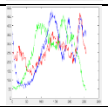
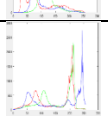
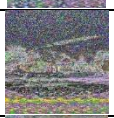
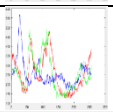
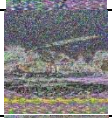
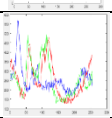
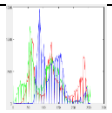
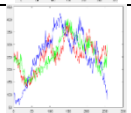
Tabel 4. Evaluation of Decipher image RGB and CMY

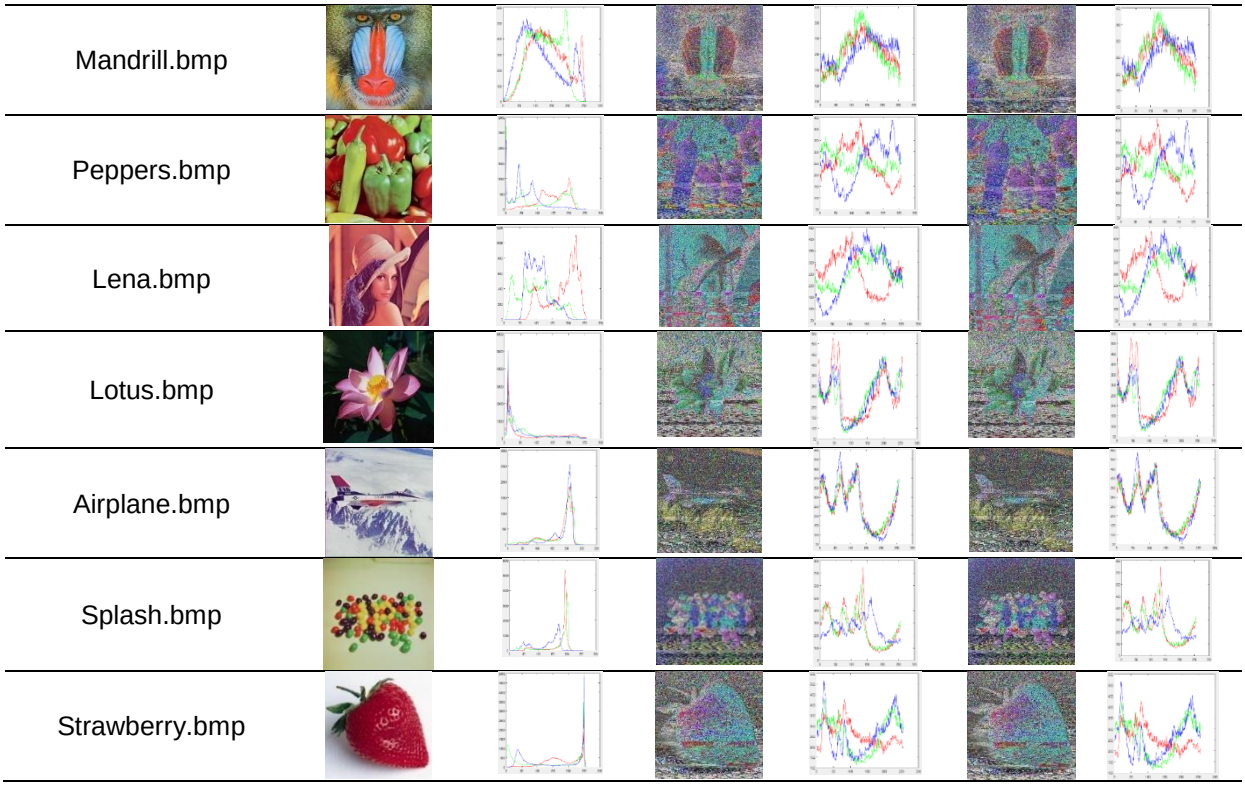
Image Name	RGB				RGB			
	MSE	PSNR	UACI	NPCR	MSE	PSNR	UACI	NPCR
Accordion.bmp	0	inf	0 %	0 %	0	inf	0 %	0 %
Cat.bmp	0	inf	0 %	0 %	0	inf	0 %	0 %

Dragonfly.bmp	0	inf	0 %	0 %	0	inf	0 %	0 %
Ferry.bmp	0	inf	0 %	0 %	0	inf	0 %	0 %
Flamingo.bmp	0	inf	0 %	0 %	0	inf	0 %	0 %
Helicopter.bmp	0	inf	0 %	0 %	0	inf	0 %	0 %
Female.bmp	0	inf	0 %	0 %	0	inf	0 %	0 %
Tree.bmp	0	inf	0 %	0 %	0	inf	0 %	0 %
Mandrill.bmp	0	inf	0 %	0 %	0	inf	0 %	0 %
Peppers.bmp	0	inf	0 %	0 %	0	inf	0 %	0 %
Lena.bmp	0	inf	0 %	0 %	0	inf	0 %	0 %
Lotus.bmp	0	inf	0 %	0 %	0	inf	0 %	0 %
Airplane.bmp	0	inf	0 %	0 %	0	inf	0 %	0 %
Splash.bmp	0	inf	0 %	0 %	0	inf	0 %	0 %
Strawberry.bmp	0	inf	0 %	0 %	0	inf	0 %	0 %

An evaluation due to check all cipher image as shown in Table 4. All cipher images in Table 4 have PSNR values <11 dB. The lowest PSNR value is in the image accordion.bmp cipher with a PSNR in RGB encryption of 5,439 dB and a PSNR in CMY encryption of 5,403 dB. Table 4 shows that the highest UACI value was generated by the cipher image accordion.bmp for RGB encryption of 44,018% and for CMY encryption of 44,312%. The highest RGB cipher image NPCR value is 99.792%, namely the cipher image from the airplane.bmp image. As for the CMY encryption results, the highest NPCR value is in splash.bmp with a value of 99,798%. The results of the decipher image evaluation for RGB and CMY images using MSE, PSNR, UACI, NPCR are shown in Table 4. Based on Table 4, it is concluded that all decipher images in the RGB and CMY color spaces have a value of MSE=0, PSNR=inf, UACI=0% and NPCR=0%, this means that the decryption result is exactly the same as the original image. So that the decryption process can be said to be perfect because the resulting decipher image has no difference at all with the original image. Evaluation using visual image and histogram has been shown in Table 5.

Table 5. Vigenere-Beaufort in RGB and CMY

Name	Original Image	Original Histogram	RGB		CMY	
			Encrypt	Histogram	Encrypt	Histogram
Accordion.bmp						
Cat.bmp						
Dragonfly.bmp						
Ferry.bmp						
Flamingo.bmp						
Helicopter.bmp						
Female.bmp						
Tree.bmp						



4. Conclusion

The combination of the Vigenere Cipher and Beaufort Cipher substitution algorithms with the Fibonacci technique can be applied to encrypt color images in RGB and CMY, with a size of 256x256 pixels and in .bmp format. The highest entropy value of the cipher image peppers.bmp is 7,991. The lowest PSNR cipher image value is accordion.bmp where for RGB it is 5,439 dB and for CMY it is 5,403 dB. accordion.bmp's highest UACI value is 44.018% for RGB and 44.312% for CMY. The NPCR value in the airplane.bmp image has the highest value in RGB of 99.792% and for CMY the highest value is in splash.bmp with a value of 99.798%. Evaluation of the decryption results shows that the decryption process can run perfectly as indicated by the values of MSE=0, PSNR=inf, UACI and NPCR=0%. Suggestions for further research are that it can be combined with other algorithms, with other file formats, and can be developed in the form of a GUI.

References

[1] F. Anwar, E. H. Rachmawanto, C. A. Sari, and de Rosal Ignatius Moses Setiadi, "StegoCrypt Scheme using LSB-AES Base64," in *2019 International Conference on Information and Communications Technology, ICOIACT 2019*, 2019. https://doi.org/10.1109/ICOIACT46704.2019.8938567

[2] C. Irawan, D. R. I. Moses Setiadi, E. H. Rachmawanto, C. A. Sari, and M. Doheir, "Hybrid Encryption using Confused and Stream Cipher to Improved Medical Images Security," in *Journal of Physics: Conference Series*, 2019, vol. 1201, no. 1. https://doi.org/10.1088/1742-6596/1201/1/012022

[3] A. Al-haj and H. Abdel-nabi, "Digital Image Security Based on Data Hiding and Cryptography," in *International Conference on Information Management Copyright*, 2017, pp. 437–440. https://doi.org/10.1109/INFOMAN.2017.7950423

[4] P. Patel and Y. Patel, "Secure and Authentic DCT Image Steganography through DWT - SVD Based Digital Watermarking with RSA Encryption," in *2015 Fifth International Conference on Communication Systems and Network Technologies*, 2015, pp. 736–739. https://doi.org/10.1109/CSNT.2015.193

[5] S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, "Data Security Using Vigenere Cipher and Goldbach Codes Algorithm," *Int. J. Eng. Res. Technol.*, vol. 6, no. 01, pp. 360–363, 2017. https://doi.org/10.17577/IJERTV6IS010245

[6] C. J. Mitchell, "On the Security of 2-Key Triple DES," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6260–6267, Nov. 2016. https://doi.org/10.1109/TIT.2016.2611003

[7] Z. E. Rasjid, B. Soewito, G. Witjaksono, and E. Abdurachman, "A review of collisions in cryptographic hash function used in digital forensic tools," *Procedia Comput. Sci.*, vol. 116, pp. 381–392, 2017. https://doi.org/10.1016/j.procs.2017.10.072

[8] Vittal Kumar Mittal | Manish Mukhija, "Cryptosystem Based on Modified Vigenere Cipher using Encryption Technique," Int. J. Trend Sci. Res. Dev. Int. J. Trend Sci. Res. Dev., vol. 3, no. 5, pp. 1936–1939, 2019.

[9] E. H. Rachmawanto, D. R. I. M. Setiadi, C. A. Sari, and N. Rijati, "Imperceptible and secure image watermarking using DCT and random spread technique," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 17, no. 4, p. 1750, Aug. 2019. http://doi.org/10.12928/telkomnika.v17i4.9227

[10] R. Naoum, A. Shihab, and S. Alhamouz, "Enhanced Image Steganography System based on Discrete Wavelet Transformation and Resilient Back-Propagation," *Int. J. Comput. Sci. Netw. Secur.*, vol. 16, no. 1, pp. 114–122, 2016.

[11] D. Sinaga, C. Umam, D. R. I. M. Setiadi, and E. H. Rachmawanto, “Teknik Super Enkripsi Menggunakan Transposisi Kolom Berbasis Vigenere Cipher Pada Citra Digital,” *Din. Rekayasa*, vol. 14, no. 1, p. 57, 2018. http://dx.doi.org/10.20884/1.dr.2018.14.1.198
[12] R. U. Marsal, F. Arnia, and R. Adriman, “Menggunakan Modifikasi Algoritma,” J. Online Tek. Elektro, vol. 3, no. 3, pp. 6–10, 2018.
[13] D. R. I. M. Setiadi, C. Jatmoko, E. H. Rachmawanto, and C. A. Sari, “Kombinasi Cipher Subtitusi (Beaufort Dan Vigenere) Pada Citra Digital,” Proceeding SENDI_U, pp. 52–57, 2018.
[14] I. L. Firdaus, R. Marwati, and R. Sispiyati, “Aplikasi Kriptografi Komposisi One Time Pad Cipher Dan Affine Cipher,” *J. EurekaMatika*, vol. 5, no. 2, pp. 42–51, 2017. https://doi.org/10.17509/jem.v5i2.9597
[15] F. Al Isfahani and F. Nugraha, “Implementasi Steganografi LSB dengan Enkripsi Base64 Pada Citra dengan Ruang Warna CMYK,” *Sci. Comput. Sci. Informatics J.*, pp. 1–8, 2019.
[16] M. A. Maricar and N. P. Sastra, “Efektivitas Pesan Teks Dengan Cipher Substitusi, Vigenere Cipher, dan Cipher Transposisi,” *Maj. Ilm. Teknol. Elektro*, vol. 17, no. 1, p. 59, 2018. https://doi.org/10.24843/MITE.2018.v17i01.P08
[17] A. Ajmera, S. S. Ghosh, and T. Vijayetha, “Secure LSB Steganography over Modified Vigenère-AES Cipher and Modified Interrupt Key-AES Cipher,” in *2018 IEEE Punecon*, 2018, pp. 1–7. https://doi.org/10.1109/PUNECON.2018.8745393