Cryptgrapy Algorithm Variably Modified Permutation Compotition (VMPC) on Image Security

Eva Sasmita [1*)], Yani Maulita[2)], Juliana Naftali Sitompul[3)]
[1,2,3)] STMIK Kaputama Binjai, Indonesia

*Coresponding Author
Email : eva_sasmita@yahoo.co.id

Abstract

The development of technology as it is today allows everyone to exchange information without any limitations of time and distance. The possibility that there will be a data leak during the information exchange process is carried out. Therefore, in sending data, especially images, aspects of security, confidentiality and efficiency of data storage are very necessary. If this important information falls into the wrong hands, it will cause unwanted things, for example image manipulation in a negative form and can harm the owner of the image. One of the methods used to maintain the security of the data is cryptography using one of the techniques, namely Vmpc. The strength of this algorithm lies in the difficulty of calculating discrete algorithms on prime integers in which multiplication operations are performed. In this study, the author encodes the image encryption with the Vmpc Algorithm to decrypt the key from Vmpc. System implementation using Visual Basic Net 2010 programming language.The results of the implementation with the initial encrypted image having a time of 4282.85 Milliseconds with randomized image results while the encrypted image will be re-decrypted which has a time of 20442.84 Milliseconds with the image results returning to the beginning.

Keywords: Cryptography, Symmetrical, Vmpc

INTRODUCTION

Image confidentiality is one of the most important aspects in information systems at this time. Due to the rapid development of science and technology that allows the emergence of new techniques, which are misused by certain parties that threaten the security of the information system. The fall of information into the hands of other parties can cause harm to the owner of the information. Digital images consist of three types, namely monocrome images (black and white/binary images), grayscale images (gray) and true color images (color images). Each color image pixel has three color elements termed RGB, namely Red (red), Green (green) and Blue (blue). Where the image is still in the form of JPG/JPEG, GIF, and Bitmap extensions. (Putra, D, 2010).

Cryptography is the science of encryption techniques where the "original text" (plaintext) is scrambled using an encryption key into a "hard-to-read random text" (ciphertext) by someone who does not have the decryption key. According to Cryptography (cryptography) comes from the Greek language which consists of two syllables, namely cryptós which means secret and gráphein which means written word. Therefore, cryptography is generally defined as secret writing. There are several definitions of cryptography in the literature. The definition in the 80s stated that cryptography is the science and art of keeping messages secure. The word art in this definition comes from the historical fact that in the early history of cryptography, everyone had a unique way of keeping messages secret. Cryptographic techniques have many algorithms in achieving the above goals, including the VMPC algorithm. (Prayitno 2017, p.2-3)

RESEARCH METHODS

The problems that will be solved by using this system are image security. In designing an image coding system that will implemented with the VMPC algorithm, first the analysis is carried out regarding the form of the system to be designed. In this research, the writer will create a system that can secure images using VMPC algorithm which aims to produce a better algorithm to prevent cryptanalysis (a party trying to find secrets (plaintext or key) of a message that has been encrypted (ciphertext) in decode in modern cryptography and help for stages system design so that satisfactory and appropriate results can be obtained with the initial design goals.

.

RESULTS AND DISCUSSION

Analysis And Design

Variably Modified Permutation Composition (VMPC) algorithm is a symmetric algorithm that modifies the RC4 algorithm. The inventor of this cryptographic system is Bartosz Zoltak published in 2004. The VMPC algorithm works in three main stages, namely Key Scheduling Algorithm (KSA), Pseudo Random Generation Algorithm (PRGA) and the Encryption and Decryption Process (Riza F *et.al* 2018)

Vmpc Algorithm Analysis

a. Key Scheduling Algorithm (KSA)

The KSA process is the process of forming an S-Box table (Table Array S) and Key (Table array [T]) which is permuted as many as 256 iterations. Pseudocode for:

```
s = 0
for n from 0 to 255: P[n] = n
for m from 0 to 767 : repeat steps 4-6:
    n = m modulo 256
    s = P[ (s + P[n] + K[m modulo c] ) modulo 256 ]
    Temp = P[n]
    P[n] = P[s]
    P[s] = Temp
Information :
P : 256-byte table of permutation storage
n, m, s : 8-bit variables
K : array to store cryptographic keys (passwords)
c: password length
```

b. Pseudo Random Generation Algorithm (PRGA) The S-Box array table will be used in this process to generate a key stream whose number is equal to the number of plaintext characters and then XOR it with the plaintext. The pseudocode for the PRGA process is:

```
n = 0
Repeat steps 3-6 throughout the plaintext:
    s = P[ (s + P[n]) modulo 256 ]
    Keystream = P[ ( P[ P[s]] + 1) modulo 256]
    Temp = P[n]
    P[n] = P[s]
    P[s] = Temp
    n= (n + 1) modulo 256
```

c. The process of encryption or decryption with XOR operations. The encryption or decryption process begins by converting each plaintext value to binary.

Encryption Process

The VMPC password is the password entered by the user. The text code used is an ASCII code (American Standard Code for Information Interchange) 256 characters (8 bits). The following is the calculation of the encryption process:

Password = [J, I, K, A]
Password = [74, 73, 75, 65] (in ASCII values)
Password will be generated with KSA and PRGA

KSA (Key Scheduling Algorithm) is one of the important elements in the algorithm, especially in the key genetering process used in data encryption algorithms.

s = 0
n = 0 to 255
P[n]:= n
P = [0, 1, 2, …, 255]
m = 0 to 767
m = 0
n = m mod 256
n = 0 mod 256 = 0
s = P[(s + P[n] + key[m mod keylength]) mod 256]
s = P[(0 + P[0]+ key[0 mod 4]) mod 256]
s = P[(0 + 0 + key[0]) mod 256]
s = P[(0 + 0 + 74) mod 256]
s = P[74 mod 256]
s = P[74] = 74
Swap(P[n], P[s])
Swap(P[0], P[74])
Swaps (0, 74)

m = 1
n = m mod 256
n = 1 mod 256 = 1
s = P[(s + P[n] + key[m mod keylength]) mod 256]
s = P[(74 + P[1]+ key[1 mod 4]) mod 256]
s = P[74 + 1 + key[1]) mod 256]
s = P[(74 + 1 + 73) mod 256]
s = P[148 mod 256]
s = P[148] = 148
Swap(P[n], P[s])
Swap(P[1], P[148])
Swaps (1, 158)

m = 2
n = m mod 256
n = 2 mod 256 = 2
s = P[(s + P[n] + key[m mod keylength]) mod 256]
s = P[(148 + P[2]+ key[2 mod 4]) mod 256]
s = P[148 + 2 + key[2]) mod 256]

s = P[(148 + 2 + 75) mod 256]
s = P[225 mod 256]
s = P[225] = 225
Swap(P[n], P[s])
Swap(P[2], P[225])
Swaps (2, 225)

m = 3
n = m mod 256
n = 3 mod 256 = 3
s = P[(s + P[n] + key[m mod keylength]) mod 256]
s = P[(225 + P[3]+ key[3 mod 4]) mod 256]
s = P[225 + 3 + key[3]) mod 256]
s = P[(225 +3 + 65) mod 256]
s = P[295 mod 256]
s = P[37] = 37

Swap(P[n], P[s])
Swap(P[3], P[37])
Swaps (3, 37)

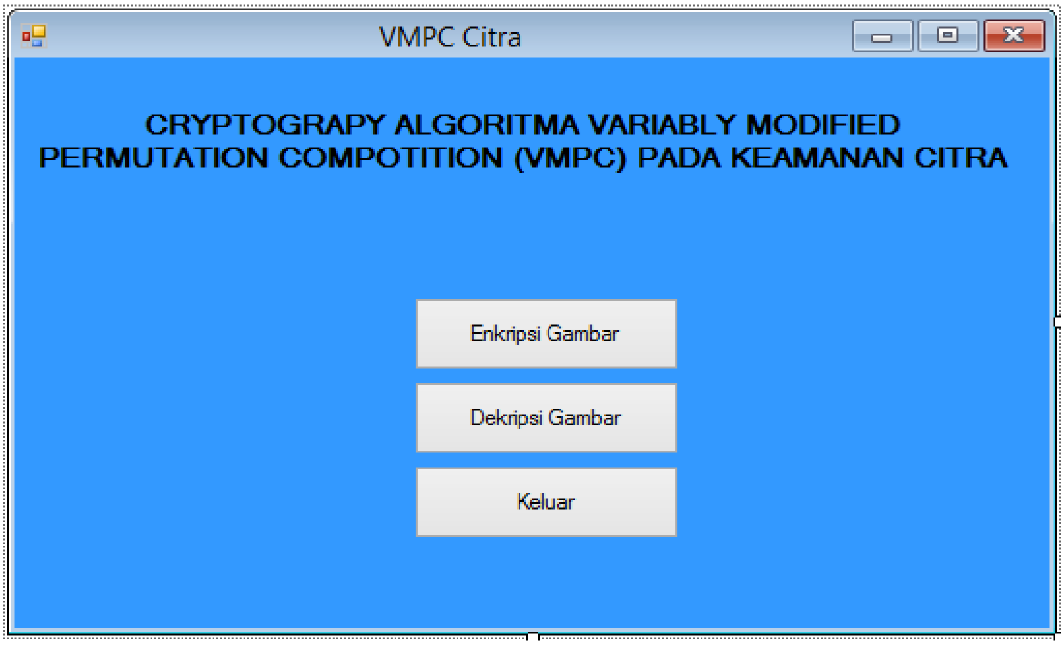
Decryption Process
From the results of encryption, the decryption process with the VMPC algorithm. Passwords will be scrambled with KSA and PRGA the same as in the encryption process. PRGA will be scrambled along the ciphertext, resulting in the same keystream as the encryption process.

Password = [J, I, K, A]
Password = [74, 73, 75, 65] (in ASCII values)
The password will be generated with KSA and PRGA so that it will produce:
Keystream = [22, 238, 40]
Plaintext = M XOR Keystream
The pixel color element values of the image are mapped back into a new image so as to produce the same image as the original image (plain image).
Then the image description process with the VMPC algorithm is as follows:
pixels (0,0) =
Red = 234 XOR 38 = 204
Green = 94 XOR 151 = 201
Blue = 91 XOR 227 = 184

pixels(0,1) =
Red = 130 XOR 82 = 208
Green = 251 XOR 55 = 204
Blue = 229 XOR 37 = 192

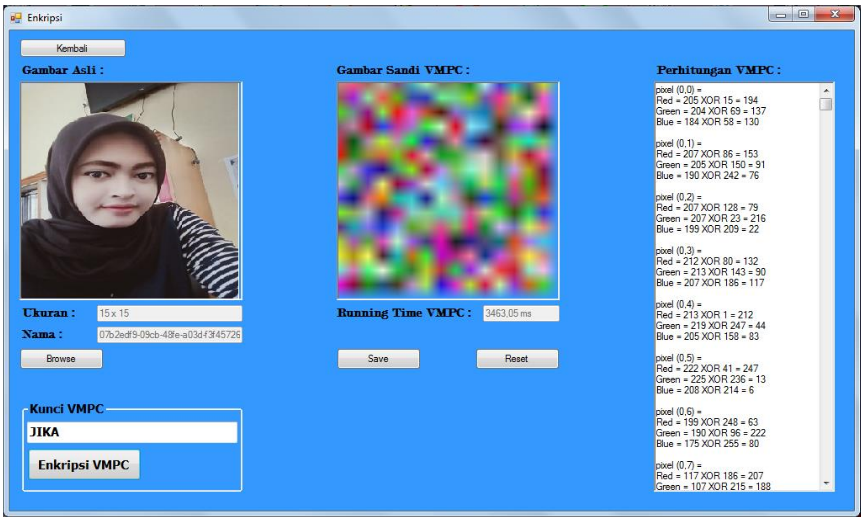
Until the Calculation reaches the pixel (14, 14)
pixels (14,14) =
Red = 52 XOR 115 = 71
Green = 169 XOR 227 = 74
Blue = 22 XOR 77 = 91

Image security applications using the VMPC method were built with the aim of keeping ownership safe from theft. This is done by encrypting the data and can be decrypted as proof of ownership of the image.(Rini, B., 2011) The encryption and decryption processes must use the same application and key. In operating this application, the user must follow the steps that have been determined so that the application works as designed. The steps of the Variably Modified Permutation Compotition (VMPC) algorithm analysis process on image security in this application can be seen below:



CRYPTOGRAPY ALGORITMA VARIABLY MODIFIED PERMUTATION COMPOTITION (VMPC) PADA KEAMANAN CITRA

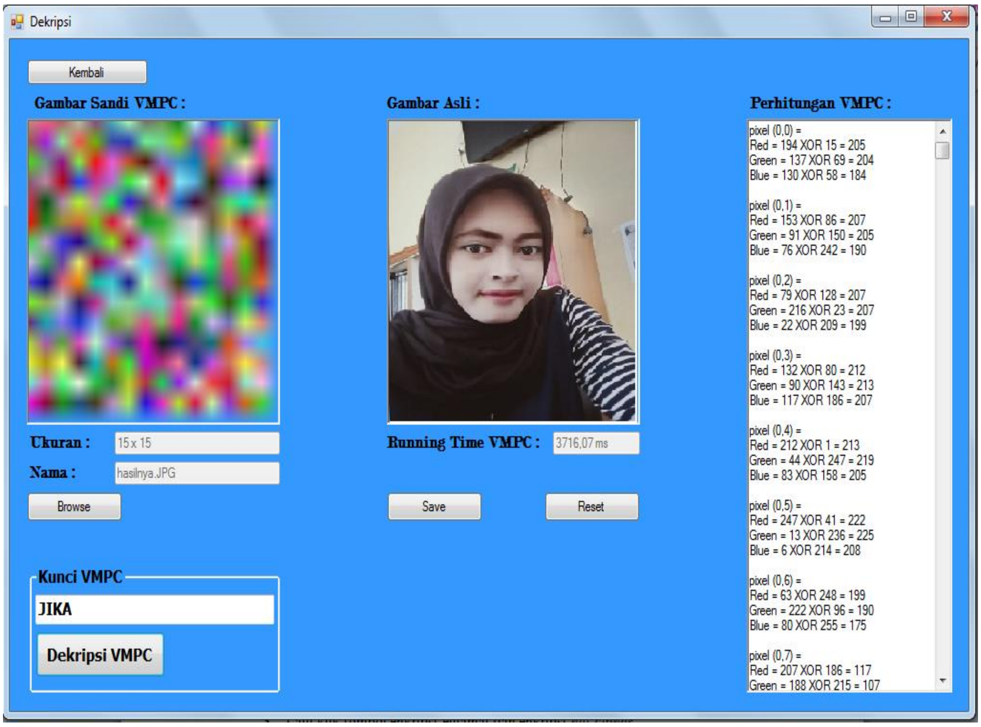
Figure.1 Main course



Ukuran : 15 x 15
Nama : 07b2edf9-09cb-48fe-a03d-f3f45726
Running Time VMPC : 3463,05 ms
Kunci VMPC: JIKA

```
pixel (0,0) =
Red = 205 XOR 15 = 194
Green = 204 XOR 69 = 137
Blue = 184 XOR 58 = 130

pixel (0,1) =
Red = 207 XOR 86 = 153
Green = 205 XOR 150 = 91
Blue = 190 XOR 242 = 76

pixel (0,2) =
Red = 207 XOR 128 = 79
Green = 207 XOR 23 = 216
Blue = 199 XOR 209 = 22

pixel (0,3) =
Red = 212 XOR 80 = 132
Green = 213 XOR 143 = 90
Blue = 207 XOR 186 = 117

pixel (0,4) =
Red = 213 XOR 1 = 212
Green = 219 XOR 247 = 44
Blue = 205 XOR 158 = 83

pixel (0,5) =
Red = 222 XOR 41 = 247
Green = 225 XOR 236 = 13
Blue = 208 XOR 214 = 6

pixel (0,6) =
Red = 199 XOR 248 = 63
Green = 190 XOR 96 = 222
Blue = 175 XOR 255 = 80

pixel (0,7) =
Red = 117 XOR 186 = 207
Green = 107 XOR 215 = 188
```

Figure.2 Main Enryption



Gambar Sandi VMPC :

Gambar Asli :

Ukuran : 15 x 15

Nama : hasilnya.JPG

Running Time VMPC : 3716,07 ms

Kunci VMPC: JIKA

Perhitungan VMPC :

```
pixel (0,0) =
Red = 194 XOR 15 = 205
Green = 137 XOR 69 = 204
Blue = 130 XOR 58 = 184

pixel (0,1) =
Red = 153 XOR 86 = 207
Green = 91 XOR 150 = 205
Blue = 76 XOR 242 = 190

pixel (0,2) =
Red = 79 XOR 128 = 207
Green = 216 XOR 23 = 207
Blue = 22 XOR 209 = 199

pixel (0,3) =
Red = 132 XOR 80 = 212
Green = 90 XOR 143 = 213
Blue = 117 XOR 186 = 207

pixel (0,4) =
Red = 212 XOR 1 = 213
Green = 44 XOR 247 = 219
Blue = 83 XOR 158 = 205

pixel (0,5) =
Red = 247 XOR 41 = 222
Green = 13 XOR 236 = 225
Blue = 6 XOR 214 = 208

pixel (0,6) =
Red = 63 XOR 248 = 199
Green = 222 XOR 96 = 190
Blue = 80 XOR 255 = 175

pixel (0,7) =
Red = 207 XOR 186 = 117
Green = 188 XOR 215 = 107
```

Figure.3 Main Decryption

.

CONCLUSION

In the picture successfully applied and able to carry out the encryption process and description. The larger the image size, the time for the encryption process and the decryption process will take longer. Test result on the system it is found that the image that has undergone the encryption process and the decryption process with the VMPC algorithm has the same information content same as the original image. Image security using the VMPC algorithm for concealing the image goes well. image has been successfully encrypted and encrypted decryption, experiments performed on the VMPC algorithm, processing time the resulting ciphertext decryption is faster than the encryption result plaintext **.**

REFERENCES

Handayono, D. R. I. M. Setiadi, Dkk. (2018). Teknik Penyembunyian Dan Enkripsi Pesan Pada Citra Digital Dan Kombinasi. Medan: Jurnal Teknik Infomatika USU.

Ermaliana, N. (2015). Format File Gambar Beserta Kelebihan. blogspot , 1-3.

Prayitno. (2017). Kriptografi 3. Yogyakarta: Andi.

Putra, D. (2010). Pengolahan Citra Digital. Yogyakarta: Andi.

Rini, B. (2011). Microsoft Visual Basic 2010 Dan Mysql Untuk Aplikasi Point Of Sales. Yogyakarta: Wahana Komputer.