Mobile and Forensics
Vol. 1, No. 1, March 2019, pp. 137-146
ISSN: 2714-6685 (online), 2656-6257 (print)
DOI: http://dx.doi.org/10.12928/mf.v1i1.XXX

Implementation of Affine Group Algebra on Digital Image Security

Rendra Soekarta[a,1*], **Miftah Sigit**[a,2]
[a]Universitas Muhammadiyah Sorong, Papua, Papua Barat, Indonesia
[1]rendrasoekarta@gmail.com, [2*]miftahsigit.rahmawati@gmail.com

Abstract

The concept of group theory has been applied to digital image security using the DES algorithm and wavelet transform. Affine Cipher algorithm was a symmetric cryptographic algorithm. This was initiated for studying further the implementation of the Affine group on the Affine transformation. More over, digital image used the Affine algorithm in security. The purpose of this paper was described the implementation of the existence of an Affine Group in the Affine transformation carried out in digital image cryptography. The concept of maintaining geometric shapes in Affine transformations and bijective nature of each Affine transformation could be formed an Affine group.

Keywords: Crypthography, Affine Transform, Affine Group, Digital Image

INTRODUCTION

Cryptography or cryptology has an important role in data and information security. Cryptography or cryptology is a mathematical theory that used in information technology. Cryptography aims that data and information cannot be read by unauthorized persons, so that information can be maintained safely. The three basic functions of modern cryptography are encryption, decryption, and keys. Cryptography is classified into three parts, there are symmetric, asymmetric, and Hash functions. Digital images as a form of digital data are currently widely used to store photos, images, or pictures in digital format. Sometimes for security reasons and privacy reasons, some people overcome it by encoding the image so that a random image is formed and cannot be seen or read by others. The DES algorithm is a symmetric standard algorithm that is still widely used [1] and still considered good in the use of digital image [2]. Simple classical encryption techniques on data are also commonly used, such as Affine transform and Hill Cipher [3][4]. Some studies, Affine Algorithm is used no longer on data but it used on images with the development of the Affine Algorithm by changing the calculation on the RGB (Red Green Blue) value [5]. Subsequent research found the security of the data contained in the steganography video by using the Affine transformation [6]. From the research mentioned, Affine Transform works on the image by maintaining the co-linearity of the default image. Previous research has found several algebraic theories on the wavelet transform, namely the form *SL(n+2, R)* which is a group [7]. Similarly, previous research applied the concept of group theory to image security using the DES algorithm and wavelet transform [8]. This gives an idea about applied theory Affine transformation and Affine algorithm to image security. The existence of group theory will be investigated by using the concepts of transformation and geometry. The problem solved is whether the Affine transformation in the Affine

Article History: *Received April 21, 2020; Revised July 8, 2020; Accepted August 10, 2020*

algorithm on image security can form a group. Furthermore, the basic concepts and properties that satisfy on Affine group in the Affine transformation will be explained.

METHODS

The approach used a qualitative approach based on literature studies from books and scientific journals, especially those related to Cryptography, Affine Algorithm, and Affine Transformation. The first step is to study the Affine algorithm used in digital security systems both algebraically. Furthermore, the connectedness of mathematical concepts in the form of mathematical functions was studied on the Affine algorithm and Affine transformations. Theoretical approach can be seen in Figure 1.

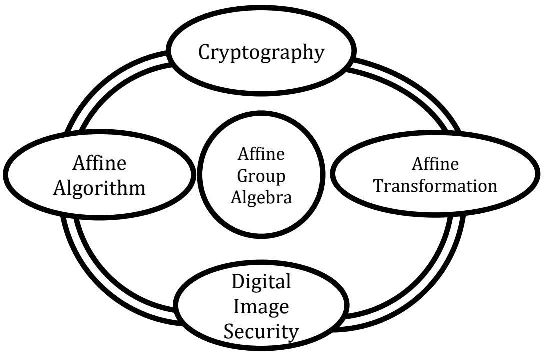

Figure 1. Theoritical approach

RESULT AND DISCUSSIONS

This article was compiled based on literature studies from various sources of books and journals on cryptography, Affine transformation, Affine Algebra, and group algebra. Several studies on cryptography and algorithms related to image data security have been carried out by many people, both from practitioners of information science and mathematics. This research continues the previous research [9] which explains the application of algebra from cryptography theory with wavelet transform. This confirms the existence of Affine group theory on wavelet transforms [10][8]. Furthermore, there is the use of Affine cipher as a key matrix in image security. Affine cipher is a cryptographic method that uses a symmetric key, which is used for encryption and descryption. Both encryption and descryption are used the same key. Affine cipher is the basis of Affine algorithm which is then used in data security on the form of images or videos. Affine algorithm with Affine cipher is a form of Affine transformation which is a one-to-one mapping. From this explanation, the idea come up to find out the implementation of Affine group algebra from cryptographic connectivity with the Affine algorithm and Affine Transformation in digital image security. Application of Affine group related to basic concepts and their properties in forming Affine transformations. Therefore, this research requires several theories as follows.

Crypthography

Cryptography is the science and art of keeping messages confidential by converting message into incomprehensible ciphers. Cryptography is used for communication security [11]. There are several cryptographic algorithms of Crypthography that can be used [12]. In this article, a classical cryptography is used, such as DES symmetric cryptography [13]. In general, classical cryptographic algorithms are grouped into two categories, namely transposition cipher and substitution cipher. Both groupings are closely related to transformation and algebra. This article uses Affine Cipher which is a special case of Substitution cipher which has the following functions:

$$e(x) = (ax + b)\ mod\ 26 \qquad (1)$$

This function is known as the Affine function

Grup

Definition (Group). A group is a set G together with a binary operation * as follow

$$G * G \ \rightarrow G$$

Satisfying the following four conditions:

1. If $a, b \in G$ then $a * beG$ (closed)
2. $a * (b * c)$ = $(a * b) * c)$ for all $a, b, c, \in G$ (assosiativity)
3. There exist an element $e \in G$ such that $a * e = a = e * a, \forall a \ \in G$ (existence of identity element)
4. For each $a \in G$ there exist $a, b \in G$ such that $a * b = b * a = e$ (Existence of an inverse for each $a \in G$)

Affine Algorithm

Affine Algorithm or Affine Cipher is a cryptographic algorithm developed from the Caesar Cipher method. Affine Cipher is a monoalphabetic cipher section where the letters in the alphabet are made into numeric form, then encrypted with a very simple mathematical function, and converted back into word characters [14]. Affine Cipher Algorithm is an algorithm that converts files from initially understood by humans into encrypted files, then inserted into storage media. The encryption process is carried out by means of character dilatation of mathematical substance. The difference from this algorithm, the dilatation done by multiplying a relatively prime number with the number used during the description process. The whole process relies on a working key and modulo. The keys used in this algorithm are two prime numbers and one integer as a slider. From the Affine function (1) with plaintext (P) multiplied by the value (b) then added to the shift (k), the encryption in the Affine algorithm can be written as

$$E(P) = (bx + k)\ mod\ 26 \qquad (2)$$

Then, the descryption can be written as

$$D(x) = b^{-1}\ mod\ 26 \qquad (3)$$

Number 26 as the sum of alphabet.

This is the same thing when performing the Affine algorithm on an image [15], the following are the steps for encryption case algorithm:

1. Determine a key matrix of size *m x m* agreed upon by the sender and receiver.
2. Perform image transformation for color images so that it become grayscale images.
3. Divide the pixel or image values into blocks, when expressed in matrix form, it have *m* row.
4. Encrypt using Affine cipher key for each matrix of each color component.

The steps for descryption case algorithm as follow:

1. Use the pre-agreed key matrix to determine the inverse matrix that will be used to decrypt the image using the Affine cipher method.
2. Process the decryption using the Affine cipher method which is same as the steps in the encryption process for each color matrix

Furthermore, in the study of the implementation of algebraic theory on the Affine algorithm, it used some functions both the encryption function and the inverse function of the description.

Affine Transform

It should be recalled that, one of interested in geometric properties invariant under transformations, for example dilatation, translations, rotations, reflection, projections, etc. Affine transform is part of geometry transformation. The Affine transformation process includes translation, rotation, scale enlargement, and cutting which are operated simultaneously. In accordance with the Affine cipher concept that has been discussed previously that the encryption and description processes are linear so that the Affine transformation is linear.

Definition (Affine Transform)

Supposed A invertible matrice 2x2 and b column vector in P ^{2}, then Affine transform defined as map $f: \mathbb{R}^2 \to \mathbb{R}^2$ such that $f(\vec{x}) = A\vec{x} + \vec{b}$.

Definition (Affine Transform)

Suppose G subset R^2, then transformation is called *Affine* on G, if $f: G \to G$ apply as

$$(x', y' = G\ ((x, y) \Leftrightarrow \frac{x' = ax + by + p}{v' = cx + dy + q}$$

with $ad - bc \neq 0$

Affine transformation does not maintain or preserve similarity. This is because the multiplier p and q are not the same.

Affine Cipher Algorithm Analysis

Affine cipher in the Affine algorithm is the development of the Caesar Cipher algorithm where the plaintext (P) is multiplied by the value (b) then added to the dilatation (k). Plaintext P whose result is ciphertext C can be encrypted with the following function:

$$C = \big((bxP) + k\big)\ modulus\ 26 \tag{4}$$

26 as length of alphabet caracter, equatin 1 for encrypsion. Then, description can use equation 2 such that becomes

$$P = b - 1(C - k)\ modulus\ 26 \tag{5}$$

As the encryption and description so that Affine cipher uses two prime numbers, b is a relatively prime number of 26. It can be concluded that the greatest common factor or gcd (b, 26) must have a result equal to 1. Some reason prime numbers are used in digital security as follows:

1. A prime number has only two factors, namely the number 1 and the prime number itself
2. The more digits of prime numbers (the bigger the prime numbers) are used, the less likely it is to solve Affine ciphers.
3. It is not easy to find the product of two factors of prime numbers.

Now consider that the binary operation $+_{26}$ on $\mathbb{Z}_{26}$ is group $(\mathbb{Z}_{26}, +_{26})$ called an abelian group, therefore the mathematical functions used in encryption and decryption are modulus groups. Then, follow as definitions obtained from the concept of the mathematical function of encryption and the description of the Affine Cipher.
Definition. Let P = C = $\mathbb{Z}_{26}$ and $K = \{(a.b) \in \mathbb{Z}_{26} x \mathbb{Z}_{26} | FPB(a.26) = 1\}$ if $K = (a, b)$ then $K \in K$ for $\forall x, y \in \mathbb{Z}_{26}$ satisfying as follow

$$Enk_k(x) = (a\,x + b)\;mod\;26 \tag{6}$$

$$Des_k(y) = a^{-1}(y - b) mod\;26 \tag{7}$$

More over, important to keep in mind the following modulus theory as below
Definition. (Integer Division Algoritm). Let a be an integer, for each $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$ then there is $\exists q, r \in \mathbb{Z}$ so that $a = am + r$
Recall from $a = am + r$ equal with), $a \equiv r(mod\;m)$, then become

$$r = a\;mod, 0 \leq r \leq (m - 1) \tag{8}$$

Integer a called quotient and integer r called remainder of division.
Definition (*Relatively Prime)*. let a and b are $(a, b) \in \mathbb{Z}^+$ integers, then a, and b are relatively prima if gcd (a, b) = 1
Definition (*Greatest Common Divisor)*. Let $(a.b) \in \mathbb{Z}, a, b \neq 0$ if a real elemen d is gcd of a and b denoted d = gcd (a,b) then
1. d|a and d|b
2. for each element c such that c|a and c|b then satisfied c|d
Greatest Common Divisor (gcd) can be formed in addition on theorem below theorem 1. Let a and b integers non zero element, there are m and n so that gcd $(a, b) = ma + nb$ Proof : Recall (6) and (7) have modulus operation form as equation (8). This gives a statement that the form of encryption and description in the Cipher algorithm are modulus operation.

Theorem 2. if a dan m with m > 1 then a and m are relatively prime, so that there is an invers a (mod m). More over, Invers a (mod m) is integer which is $\bar{a}a \equiv 1(mod\;m)$
Proof : It clearly said that pair of a and m are relatively prime so that gcd (a,m) = 1. Namely integer x for a(mod m) then integer x' for invers x so that x'x=1. Thus, x'(a mod m)=1. Then, recall definition gcd and theorem 1 of modulus theory.
Suppose $x' = \bar{a}\;(mod\;m)$ then

$$\begin{gathered}\big(\bar{a}(mod\;m)\big)(a(mod\;m) = 1\\ \Leftrightarrow \bar{a}a\;(mod\;m) = 1\\ \Leftrightarrow \bar{a}a \equiv 1\;(mod\;m)\end{gathered}$$

The encrypsion sould be preserve in concruency. To complicate the frequency analysis in security when its cryptograph so it use set which are relatively prime. Thus, the key of Affine cipher in equation (3) consist of two parameter note a and b. Then, invers a note a^{-1}. More over a must apply gcd (a,26) = 1
Proposition. Let $e = (ax + b)\;mod\;26$ with $p = (ax + b)$ for $\forall p \in \mathbb{Z}_{26}$ and $a, x, b \in \mathbb{Z}^+$ then $e^{-1} = a^{-1}(y - b)\;mod\;26$
Proof: there are some condition of modulus operation on integers, such as a (mod m) with gcd (a,m) =1 for each a,m positively integers, m > 1 then pair a and m are relavely prime. Relate to definition, let p as integer so both p and 26 are relatively prime. Its clearly that $gcd\;(p, 26) = 1$, there is $m, n \in \mathbb{Z}_{26}$ so that $mp + n(26) = 1$ implied that

$$mp + n(26) \equiv 1(mod) \tag{9}$$

Because $n(26) \equiv 0\ (mod\ 26)$ so there is no remainder of division. Thus,

$$mp + n(26) \equiv 1\ (mod\ 26)$$
$$\Leftrightarrow mp\ \equiv 1\ (mod\ 26) \qquad (10)$$
$$p^{-1} = a^{-1}(x - b)$$

Suppose inverse $e\ =\ e^{-1}$ then inverse $p\ (mod\ 26)\ =\ e^{-1}$ so that $e^{-1}\ p =\ 1\ (mod\ 26)$. Since $p \in \mathbb{Z}_{26}$ it follows that

$$e^{-1} = p^{-1}(mod\ 26)$$
$$\Leftrightarrow m = p^{-1}(mod\ 26)$$

Recall equation (10) then,

$$\Leftrightarrow m = a^{-1}(x - b)(mod\ 26)$$

with $p = ax + b$
That result give an explanation, the inverse $e\ is\ p\ (mod\ 26)$ denoted as function on Affine Cipher algorithm.

Begin with number of alphabet on Affine Cipher, note that ($\mathbb{Z}_{26}$,*) with binary operation defined as $a * b = 2_a + b$, then

1. Let $a, b \in \mathbb{Z}_{26}$ because $a, b \in \mathbb{Z}_{26}$ and $a * b = 2_a + b \in \mathbb{Z}_{26}$ then $2_a + b \in \mathbb{Z}_{26}$ (closed)
2. Let $a, b, c \in \mathbb{Z}_{26}$ then
   $a \star (b \star c) = (a \star b) \star c$
   $a \star (b \star c) = a \star (2b + c)$
   $= 2a + (2b + c)$
   $(a \star b) \star c = (2a + b) \star c$
   $= 2(2a + b) + c$
   $= 4a + 2b + c$

$2a + (2b + c) \neq 4a + 2b$ so that $a \star (b \star c) \neq (a \star b) \star c$ (not assosiative)
In Algebra, it possibly to said that this is can be formed a group called quasigroup. Unfortunately, it is not discussed in this article. So, recalled the definition of group such that *($\mathbb{Z}_{26}$,*)* is not group. In other words, *Affine Cipher* for the encryption with modulus $\mathbb{Z}_{26}$ on binary operation * is not group. This result can be said that affine cipher with modulus Z_{26} on binary operation * is not included in affine group.

Furthermore, *Affine Cipher* for the encryption can be formed by mathematics function. This will be shown that the mathematical function of Affine Cipher encryption maintains linear properties with bijective maping
Let f be function $f: \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}$ $\quad f(x) = (ax + b)\ mod\ 26$ defined as for each $x \in \mathbb{Z}_{26}$ and $a, b \in \mathbb{Z}$

1) Show that f is injective function
   let $x_1, x_2 \in \mathbb{Z}_{26}$ such as $f(x_1) = f(x_2)\ f(x_1) = (ax_1 + b)mod\ 26$
   so that $f(x_1) = (ax_1 + b)mod\ 26$and $f(x_2) = (ax_2 + b)mod\ 26$
   because $f(x_1) = f(x_2)$
   then,

$ax_1 + b)mod\ 26 = (ax_2 + b)mod\ 26$
$\Leftrightarrow ax_1 = b = ax_2 + b$
$\Leftrightarrow ax_1 = ax_2$
$\Leftrightarrow x_1 = x_2$

Clearly, f is injective so that for each $x_1, x_2, \in \mathbb{Z}_{26}$ if $f(x_1) = f(x_2)$ then $x_1 = x_2$

2) show that f is surjective function
Let $z \in \mathbb{Z}_{26}$ there is $x \in \mathbb{Z}_{26}$ such that $z = (ax + b) mod\ 26$
As defined as function, so that $\mathbb{Z} = f(x)$
Clearly, f is surjective

From the proof of 1) the injective function and 2) the surjective function, the mathematical function of Affine Cipher's encryption is bijective. This shows that Affine Cipher is simetry and linearity

Affine Transform Analysis

The process of point space transform on Euclide with vector space in mathematics can be done through Affine transformation [16]. The reason for using affine transform to security images is about the geometric properties. Atleast, the point space is transformed with vector space can be preserved. After analyzing the existence of a group in the Affine Cipher with certain conditions, conclude that the nature of the binary operation to the Affine transformation can formed a group. Affine transformation can be expressed in the form of a matrix, namely a square matrix with a binary multiplication operation. Several theories have proven that square matrices with multiplication operations can form groups. Therefore, this article explain the formation of Affine group from Affine Transformation. In this case, the Affine transformation is denoted in the form of Seitz notation where f is a linear function and $\vec{t}$ is a translation vector. The function f has linear properties so that it none other than the Affine Cipher previously discussed. Then, the multiplication of the Affine transformation is defined as follows:

$$\{f|\overrightarrow{t_1}\}.\{g|\overrightarrow{t_2}\} = \{fg|\overrightarrow{t_2}\}.\{g|\overrightarrow{t_1}\}$$

This can be shown that the binary multiplication of the Affine transformation function forms a group. It is clearly that the binary multiplication operation is closed from this definition. Since f is a linear function, there is inverse $\{f|\vec{t}\}$ called $\{f|\vec{t}\}^{-1}$ such that $\{f|\vec{t}\}^{-1} = \{f^{-1}| - f^{-1}\vec{t}\}$ and identity element e so that $e = ff^{-1}$, then

$$\{f|\vec{t}\}.\{f|\vec{t}\}^{-1} = \{f|\vec{t}\}.\{f^{-1}| - f^{-1}\vec{t}\}$$

$$\Leftrightarrow \{f|\vec{t}\}.\{f^{-1}|-f^{-1}\vec{t}\} = \{ff^{-1}|f\vec{t} + (-f^{-1}\overrightarrow{t}\}$$

$$\Leftrightarrow \{e|(f - f^{-1})\vec{t}\}$$

Suppose $(f - f^{-1})\vec{t} = \vec{t}'$ so that $\{e|(f - f^{-1})\vec{t}\} = \{e|\vec{t}'\}$
Noted $\{e|\vec{t}'$ which is an identity element. Thus, recall the multiplication operation to show the properties of the associative.

$$\{f|\vec{t}\}.\{e|\vec{t}'\}.\{f|\vec{t}\}^{-1} = \{f|\vec{t}\}.\{e|\vec{t}'\}.\{f|\vec{t}\}^{-1}$$

$$\Leftrightarrow \{fe|f\vec{t} + \vec{t}'\}.\{f^{-1}| - f^{-1}\vec{t}\}$$

$$\Leftrightarrow \{fef^{-1}|fe\vec{t}' + -f^{-1}\overrightarrow{t}\}$$

$$\Leftrightarrow \{f|\vec{t}\}.\{ef^{-1}|e\vec{t}' + \vec{t}\}$$

$$\Leftrightarrow \{f|\vec{t}\}.(\{e|\vec{t}'\}.\{f|\vec{t}\}^{-1}\vec{t}\})$$

$$\Leftrightarrow \{f|\vec{t}\}.(\{e|\vec{t}'\}.\{f|\vec{t}\}^{-1})$$

Therefore, the Affine transformation is a group which is formed to the Affine group.

Affine Group

Let $Aff(n)$ be a group notation formed the Affine transformation. This paper tries to form an Affine group on R^n, because it works in image security. The thing to remember is that the image is locked with encryption and a description of the Affine Cipher function, then maintains Affine congruence. In preserve congruence, it is necessary to transform Affine with linear and bijective nature. The Affine transform also maintains parallel lines in the image. Mostly, Affine transforms used in image security are invertible square matrix spaces. Some of the Affine transformations used in cryptography in the image can be written as follows:

$$F(\theta)=\begin{bmatrix}\varphi(x,y)\cos[\vartheta(x,y)] & -\vartheta(x,y)\sin[x,y] \\ \frac{\sin[\vartheta(x,y}{\varphi(x.y)} & \frac{\cos[\vartheta(x,y}{\vartheta(x,y)}\end{bmatrix}$$

the invers matrix can be expressed as follow

$$F^{-1}(\theta)=\begin{matrix}\frac{\cos[\vartheta(x,y)]}{\varphi(x,y)} & \varphi(x,y)\sin[\vartheta(x,y)] \\ \frac{\sin[\vartheta(x,y)}{\varphi(x,y)} & \varphi(x,y)\cos[\vartheta(x,y)]\end{matrix}$$

function $\vartheta(x,y)$ and $\varphi(x,y)$ are any real number matrix with same size. Thus, affine transform can be written as augmented matrix

$$\begin{bmatrix}x' \\ y' \\ 1\end{bmatrix}=\begin{bmatrix}a & b & p \\ c & d & q \\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}x \\ y \\ 1\end{bmatrix}$$

(x,y) as point which is the starting location of an image (pixel) and (x',y') as point which is the location after doing Affine transform. In other word, function $a: R^3 \rightarrow R^3$ so that $x' = Ax + by + p$ for each $a, b \in R^3$ and A invertible matrix is affine transform. So it can be said that the Affine group denoted as $Aff(n)$ is a group of Affine transforms on Rn defined as follows

Definition. For each $v \in R^n$ such that $T_v: R^n \rightarrow R^n$ is translation along v with $T_v(x) = v + x$ for any $x \in R^n$ then sets of translation isomorphic with group $(R^n, +)$. Thus, the isomorphic sets of R^n forms $GL_n = \{A \in R^n: \det\,(A) \neq 0\}$ which is homomorphic. So that, the multiplication of $R^n x GL_n$ can be formed *Affine* group.

Example of Affine Group

Groups of orthogonal matrices which are square matrices and it have the same properties inverse matrix as the transpose matrix.

CONCLUSIONS

The Affine Cipher function used in the Affine Cipher algorithm is matrix multiplication and vector addition. Affine transformation on image security is used to maintain geometric properties. As a result, the image mapped by the Affine transformation can be maintained in its dimensional aspect. One of these aspects is in the form of collinearity obtained from the translation process. Affine Transformation is bijective which can be formed an Affine Group. The set of linear transformations that have Affine properties, then the Affine Group will be found in the transformation set.

REFERENCES

[1] A. Yosanny, “Perancangan Enkripsi Pada Citra Bitmap Dengan Algoritma Des, Triple Des, dan Idea,” *ComTech Comput. Math. Eng. Appl.*, vol. 1, no. 2, p. 853, 2010, doi: 10.21512/comtech.v1i2.2618.

[2] S. El-Zoghdy, Y. Nada, and A. Abdo, “How Good Is The DES Algorithm In Image Ciphering?,” *Int. J.*, vol. 803, no. February, pp. 796–803, 2011, [Online]. Available: http://ijana.in/papers/v2i5-1.pdf.

[3] M. Toorani and A. Falahati, “A secure cryptosystem based on affine transformation,” *Secur. Commun. Networks*, vol. 4, no. 2, pp. 207–215, 2011, doi: 10.1002/sec.137.

[4] E. S. Pasaribu, “Penerapan Aritmatika Modulusdan Matriks dalam Cipher Hill,” 2012.

[5] M. L. Wijaya, K. Yulianti, and H. S. Husain, “Kriptografi Dengan Komposisi Caesar Cipher Dan Affine Cipher Untuk Mengubah Pesan Rahasia,” *J. EurekaMatika*, vol. 5, no. 1, pp. 30–45, 2017.

[6] M. Ramalingam, N. A. Mat Isa, and R. Puviarasi, “A secured data hiding using affine transformation in video steganography,” *Procedia Comput. Sci.*, vol. 171, no. 2019, pp. 1147–1156, 2020, doi: 10.1016/j.procs.2020.04.123.

[7] A. Nag *et al.*, “Image encryption using affine transform and XOR operation,” *2011 - Int. Conf. Signal Process. Commun. Comput. Netw. Technol. ICSCCN-2011*, no. Icsccn, pp. 309–312, 2011, doi: 10.1109/ICSCCN.2011.6024565.

[8] M. S. Rahmawati and R. Soekarta, “Teori Grup Pada Algoritma DES Dan Transformasi Wavelet Diskrit Dalam Program Aplikasi Keamanan Citra Digital,” *Insect (Informatics …*, vol. 4, no. 1, 2019, [Online]. Available: http://ejournal.um-sorong.ac.id/index.php/insect/article/view/281.

[9] M. S. Rahmawati and R. Soekarta, “Penerapan Aljabar Linear pada Transformasi Wavelet Diskrit dalam Program Aplikasi Keamanan Citra Digital,” in *SEMINAR MATEMATIKA DAN PENDIDIKAN MATEMATIKA UNY*, 2019, pp. 1–6.

[10] Q. Qin and N. Wang, “Wavelet transform associated to the affine group AGmp,” *Approx. Theory its Appl.*, vol. 11, no. 4, pp. 45–50, 1995, doi: 10.1007/BF02836829.

[11] S. A. Babu, P. Analyst, and R. Technologies, “Modification Affine Ciphers Algorithm for Cryptography Password,” *Int. J. Res. Sci. Eng.*, vol. 3, no. 2, pp. 346–351, 2017.

[12] B. Y. Chong and I. Salam, “Investigating deep learning approaches on the security analysis of cryptographic algorithms,” *Cryptography*, vol. 5, no. 4, 2021, doi: 10.3390/cryptography5040030.

[13] Baha Eldin Hamouda Hassan, “Comparative study of different cryptographic algorithms,” *J. Inf. Secur.*, vol. 11, pp. 138–148, 2020, doi: 10.4236/jis.2020.113009.

[14] A. B. Nasution, “MODIFIKASI ALGORITMA AFFINE CIPHER UNTUK,” *(Jurnal Teknol. Inf.*, vol. 4, no. 2, pp. 377–382, 2020.

[15] M. Kharolina, “Implementasi Algoritma Affine Cipher Pada Citra Menggunakan Binomial Newton Sebagai Matriks Kunci,” *Pelita Inform. Budi Darma*, vol. XVI, no. 1, pp. 52–54, 2017.

[16] J. Gallier, “Basics of Affine Geometry,” *Geom. Methods Appl.*, vol. 38, pp. 7–63, 2011, doi: 10.1007/978-1-4419-9961-0_2.

AUTHORS BIBLIOGRAPHY

RENDRA SOEKARTA, Lahir di Pare-pare pada tanggal 19 Januari 1079. Penulis menyelesaikan gelar Sarjana pada tahun 2003 di STMIK DIPANEGARA dengan bidang Sistem Informasi, selanjutnya menyelesaikan gelar Magister di tahun 2011 di Universitas Hassanudin. Saat ini penulis menjadi dosen Teknik Informatika di Universitas Muhammadiyah Sorong dan telah menulis beberapa artikel.

MIFTAH SIGIT RAHMAWATI, lahir di Klaten pada tanggal 19 September 1986. Pada tahun 2005 menjadi lulusan SMA Negeri 1 Klaten, dan melanjutkan kuliah S1 di Universitas Negeri Yogyakarta dengan jurusan Pendidikan Matematika. Penulis memperoleh gelar Sarjana nya pada tahun 2009 dan melanjutkan studinya S2 di Universitas Gadjah Mada dengan jurusan Matematika Aljabar Dalam tesisnya menuliskan tentang Fuzzy SubGrup. Setelah memperoleh gelar Magister pada tahun 2012, penulis mengabdikan diri di Universitas Muhammadiyah Sorong sebagai Dosen Teknik Informatika pada tahun 2014 sampai sekarang. Beberapa artikel yang telah ditulis terkait kriptografi, pendidikan, dan teori Grup.