
Analysis Security of Absence Information System with Finger Print using Minutiae Method on STEKOM

Laksamana Rajendra Haidar¹, Haris Ihsanil Huda², Bagus Sudirman³

¹Universitas STEKOM

Jalan Majapahit no 605 Semarang e-mail: laksamanahaidar@stekom.ac.id

²Universitas STEKOM

Jalan Majapahit no 605 Semarang e-mail: haris@stekom.ac.id

ARTICLE INFO

Article history:

Received 30 November 2021

Received in revised form 2 December 2021

Accepted 10 December 2021

Available online 31 December 2021

ABSTRACT

Employee attendance is primary factor at an institution or company in achieving target. This condition relates to disciplines. And affect to pros and cons company management or human resource quality it self, impact that happened can be in the form of lack of output from production result. Much

company managements take decision by conduct salary amputation of each absence employee in the operation. In consequence, must existence of special record to note existence and employees absence in order to employees existence in conducting job activity are noted properly. A lot of way of used for processing employees attendance, one of that is with use barcode machine. In STEKOM, absence system which used is fingerprint scanner machine, but the system mentioned is requiring expensive cost enough, it needs troubleshooting and also repairing. So that company have to releasing a lot of cost for handle employees attendance process. Beside that, damage fingerprint condition, wet and dirty can be became of employees. So its disturb process of absence transaction. Minutiae method is a method which is used by the writer in this research. This method is assumed as an effective method to describe the intrinsic elements in designing and identifying finger print. It is because in processing a program, it should be described in order to be understandable.

Keywords: Security, Finger Print, Absence, Minutiae

1. INTRODUCTION

Biometrics technology is a new technology that has a primary function to recognize humans through fingerprints, eyes, face, or other body parts. Biometrics comes from the word bios, which means life, and metron, which means size. Biometrics is a technology to recognize a person uniquely. Fingerprint is a tool that can read a person's fingerprint and know who the owner of the fingerprint, so will fingerprint data owner out is in accordance with the data that has been in input first.

Weaknesses that exist in this system is Old systems can make things easier Cheating employees who want to Forged his absence signature, The existence of making the absenteeism Constantly and must be deposited To the head of the relevant agency for Checked, as well as additional fees For the purchase of attendance papers.

Human fingerprints are so unique that no one has identical fingerprints to anyone, even between siblings or twins. Fingerprints have proven to be quite accurate, safe, easy and comfortable when compared to other human identification recognition systems. Uniquely the ten fingers of each person is different. Being aware of this fact, the use of fingerprints for employees can be a better way of presenting solutions because with fingerprints there is no longer the term "titip absent". In an effort to achieve better work productivity, important attendance factors, especially those related to discipline, Payroll labor and work performance. Employee Presence is one important factor in human resource management, for that STEKOM need a computerized system to process data attendance better. It is needed more attention and handling so that problems can be solved. So the performance of every employee in STEKOM can be more effective. The purpose of this journal is to analyze the methods used in security systems that use fingerprints as well as provide solutions in selecting tools to protect and protect critical data and information.

2. LITERATURE

2.1. Biometric System

The use of one's identification using fingerprint reading, retina of the eye on a retina scan, and another is to maintain the security of a place or object. The use of limbs as an input for the identification of a person in security is called the use of a biometric system. The biometric system is the study of automated methods for recognizing human beings based on one or more parts of the human body or the behavior of the human being itself which has its uniqueness. The main purpose of the use of biometric systems is to preserve the authenticity of key uniqueness, since it is almost impossible to read the input of fingerprints or retinas of different people resulting in the same reading result. The three basic patterns of fingerprints are arches or archs, loops, and circles or whorls.

- Arch is a pattern in which the pattern enters from one side of the finger, rises to the middle forming an arc, and then out from the other side of the finger.
- Loop is a pattern where the wrinkles enter from one side of the finger, curve-shaped, and tend to come out of the same side when entering.
- Whorl or circular-shaped circular pattern like the mid-point mountains of a finger. Scientists have also found that family members often share fingerprints with the same general pattern, which leads to the belief that these patterns are inherited

The use of biometric systems allows the uniqueness to keep the security of a place or thing. This led to the idea of combining biometric systems and one of the cryptographic algorithms, discussed in this journal is the classical cryptographic algorithm. In this journal, the discussion is limited to the biometrics of the fingerprint, so the hardware used is the fingerprint reader, the method used in accordance with the results of fingerprint biometrics reading.

2.1.1. Characteristic of Fingerprint

Identification by fingerprints also has certain pattern characteristics, there are three archetypal characteristics, ridge ending, bifurcation, point, and island. And here are the variations of the four basic characters

2.1.2. Minutiae Method

The principle of fingerprint imaging processing using fingerprint reader is quite complicated, but already the amount of hardware used to make the constraint becomes blurred. These imaging principles among others are pattern based and minutiae based. In pattern based fingerprint recognition, fingerprint patterns are grouped into 3, namely arch, Loop and whorl. While on minutiae based there are also 3 classification pattern that is ridge ending, bifurcation, and dot (short ridge). To fulfill the appropriate block length; Usually padding is done on the last plaintext block. The last block of bada padding can be done in various ways, for example by adding certain bits. One example of applying padding is by adding the total number of padding as the last byte in the last plaintext block. For example the block length is 128 bits (16 bytes) and in the last block it consists of 88 bits (11 bytes) so that the required padding number is 5 bytes, that is by adding a 4 byte zero, then adding the number 5 by one byte. Another way can also use the addition of eof file characters in the last byte and then given padding afterwards. Decryption is the reverse process of

the encryption process, changing the ciphertext. Back into the plaintext form. To remove the padding given at the time of encryption, it is done . Based on the amount of padding information that is the number in the last byte.

The underlying mathematical basis of the encryption process and the description is the relation between two sets ie that contains the plaintext element and that contains the ciphertext element. Encryption and decryption is a function of transformation between the sets. If the plaintext elements are denoted by P, ciphertext elements are denoted by C, while for encryption the process is denoted by E, decryption with notation D, then the mathematical cryptographic process can be expressed as follows:

$$\text{Encryption: } E(P) = C \quad \text{Decryption: } D(C) = P \text{ or } D(E(P)) = P$$

In the conventional encryption scheme or symmetric key a key is used to perform the encryption process and decryption. The key is denoted by K, so the cryptographic process is:

$$\begin{aligned} \text{Encryption: } EK(P) &= C \\ \text{Decryption: } DK(C) &= P \text{ or } DK(EK(P)) = P \end{aligned}$$

While the asymmetric key system used public key (key) for encryption and private key (private Key) for the decryption process so that both processes can be expressed as follows:

3. RESEARCH METHOD

In the minutiae matching stage, corresponding minutia pairs between template and query images are determined by comparing local neighborhoods of minutia points. The local neighborhood of a minutia is typically represented using a fixed number of its nearest minutiae. However, due to the lack of minutiae, those typical representations of local neighborhood cannot be discriminative in partial fingerprint images. To make the local neighborhoods more discriminative, the local neighborhood, also referred to as the local structure in

this paper, is newly described using both the adjacent minutiae and the RSFs of a central minutia. The nearest neighbors of a certain minutia may vary in partial fingerprint images even captured from the same finger when the overlapped region of two images is very small. Therefore, the local structure in our work contains all minutiae and RSFs within the given ranges from a central minutia. Note that the ranges for neighboring RSFs and minutiae are defined differently ($R1 = 40$ and $R2 = 80$, respectively in this paper). This is because many more RSFs are included in a small local region compared with minutiae.

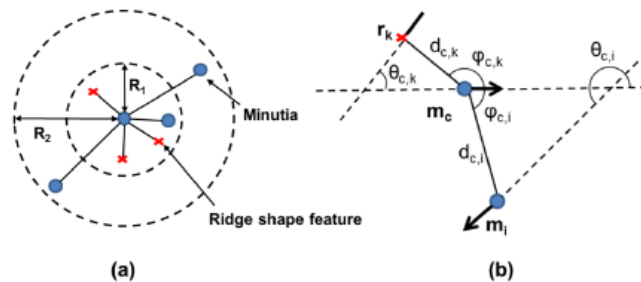


Figure 1 Minutiae Method

As illustrated in Fig. 7(b), given a central minutia M_c , its neighbor N_k (which can be either a minutia or a RSF point) is represented by the Euclidean distance $d_{c,k}$ between the minutiae M_c and N_k , the orientation difference $\theta_{c,k}$ between M_c and N_k , the directional difference $\phi_{c,k}$ between the direction of M_c and the direction of the edge connecting M_c to N_k , and the t_k of N_k (ending or bifurcation for a minutia, and concave or convex for a RSF). Then, the local structure of M_c is defined as $L(M_c) = \{(d_{c,k}, \theta_{c,k}, \phi_{c,k}, t_k)\}$, where N_k is the total number of adjacent minutiae and RSFs.

Let $L(m^T)$ and $L(m^Q)$ be the local structures of a minutia m^T in the template fingerprint image and a minutia m^Q in the query fingerprint image, respectively. These two local structures are matched by

dynamic programming. Dynamic programming finds the optimal matching result that maximizes the similarity score between $L(m^T)$ and $L(m^Q)$

$$S_m(m^T, m^Q) = \frac{S_m(m^T, m^Q) + S_r(m^T, m^Q)}{2}, \dots \dots \dots (\text{formula 3.1})$$

where $S_m(m^T, m^Q)$ and $S_r(m^T, m^Q)$ are the similarities computed by matching neighboring minutiae and by matching neighboring RSFs, respectively. The similarities are calculated by the following equation

$$S_m(m^T, m^Q) = \frac{2 \sum F_s(ni^T, ni^Q)}{N^T + N^Q}, \dots \dots \dots (\text{formula 3.2})$$

where ni^T, ni^Q represent the total number of neighbors (minutiae or RSFs) in $L(m^T)$ and $L(m^Q)$ respectively, and $F_s(ni^T, ni^Q)$ represents a matching certainty score between ni^T and ni^Q , which are local neighbors in $L(m^T)$ and $L(m^Q)$ respectively. The matching certainty score between ni^T and ni^Q is calculated by comparing their topological relation (relative distance, orientation difference, directional difference, and type) to the central minutiae as follows

4. RESULT AND ANALYSIS

4.1 Process Verification

Minutiae points are a kind of point formed on the fingerprint. There are several types of minutiae or can also be called a ridge, including ridge ending, ridge crossing, and small features formed from ridge fingerprinting on fingerprints called ridge bifurcation. Figure 6 shows the shape of the fingerprint minutiae. Verification is a matching process similar to identification only in the verification process, the fingerprints are matched one by one in which each fingerprint insert is compared with a particular fingerprint template Saved before. The output of the program is whether the verification process succeeds or fails.

Image Improvement

The first stage is the processing of fingerprint images. At this stage the fingerprint image of the scanning results will be improved Quality through several processes.

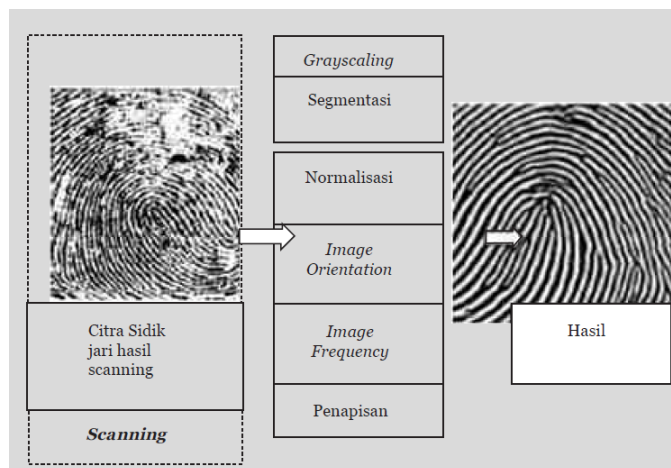



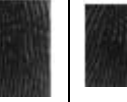




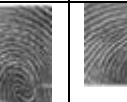






Figure 2 Verification Process

Convert a color image to a black-and-white image by averaging the values of all three color elements per pixel. Segmentation is the process of separating objects in an image from the background area. After that the segmented image is normalized by standardizing the intensity value of an image by adjusting the gray level coverage so that it is within the scope of the expected value. Image Orientation and Image Frequency process is used for fingerprint image screening process. The screening used is the screening of gabor.

Ekstraktion Minutiae

Simulated Device	Cropped Sample				
FVC 2002					
Sensing Area(mm ²)	9.8 x 9.3	8.1 x 7.7	6.9 x 6.5	9.3 x9.3	7.7 x7.7
Image Size(pixel)	192 x 184	160 x152	136 x 128	184 x 184	152 x 152
FVC 2002					
Sensing Area(mm ²)	9.3 x 9.3	7.7 x 7.7	6.9 x 6.9	9.3 x9.3	7.7 x7.7
Image Size(pixel)	184 x 184	152 x152	136 x 136	184 x 184	152 x 152
BERC					
Sensing Area(mm ²)	9.8 x 9.8		8.1 x 8.1		7.3x 7.3
Image Size(pixel)	192 x 192		160 x 160		144 x 144

There are three stages in this Image Extraction, including: Binaryzation, Decimation of pattern and detection of minutiae. Image conversion in the binary process is done by the operation of the mining so that the existence of the object in the form of fingerprint stroke. Pattern screening aims to reduce unnecessary parts. Then the image of minutiae detected by using crossing number method. The minutiae points are detected by scanning the local neighbors on each pixel ridge in the image using the 3 x 3 window size. Then the crossing number value is calculated, which is defined as half the sum of the differences between the adjacent pixel pairs in the eight-neighborhood



Figure 3 Menu Application of Absence

DATA MASTER KARYAWAN


NOMOR INDUK:

NAMA KARYAWAN:

ALAMAT RUMAH:

TANGGAL LAHIR:

TANGGAL MASUK:





NO	INDUK	NAMA KARYAWAN	ALAMAT KARYAWAN	TGL LAHIR	TGL MASUK
▶	T1651	ADE NUGRAHA	SEMARANG	20/03/4917	
	WLR10	AHMAD ASHIFUDD	REMBANG	24/01/4835	
	WLR44	BAGUS INDRAMAN	KALIWUNGU	20/06/1997	
	WLR13	BAGUS SUDIRMAN	PATI	27/08/1990	
	WLR07	BOBI	TUNTANG CITY	07/01/1988	
	T2345	CANDRA SUPRIADI	KALIBANTENG		
	WLR77	EDY SISWANTO	CITRA HARMONI 12	01/03/2008	
	WLR87	EKO SISWANTO	DEMAK	12/10/1987	
	WLR99	HARIS IHSANIL HUI	KENDAL	20/04/1988	
	WLR95	LAKSAMANA RAJEN	JEPARA	22/02/4917	
	WLR01	MIFTAHURROHMAI			
	WLR30	MOH. MUTHOHIR	JL SURGA	08/08/2018	
	WLR66	MUNIFAH	KALIWUNGU	06/06/1985	
	WLR31	PURRI PRATIWI	KENDAL	31/01/1987	
	WLR12	SUKEMI KAMTO SU			
	WLR02	SUPRIYANTO	TEMBALANG	23/07/4725	
	WLR06	TEGUH SETIADI	PATI	01/11/2014	

Figure 4 Register data

Figure 5 Input data Register

22-06-2017
Kamis
14:14:59





NAMA	TANGGAL	PAGI	SIANG	SORE	MALAM	
▶	TEGUH SETIADI	Thursday 22 June 2017	7:42:37	13:15:31	15:47:34	20:42:34
	TEGUH SETIADI	Wednesday 21 June 2017	7:35:19	13:09:40	15:35:08	20:45:14
	AHMAD ASHIFUDDIN AQHAM	Wednesday 21 June 2017	7:58:27	13:04:11	15:47:23	20:31:22
	SUKEMI KAMTO SUDIHYO	Wednesday 21 June 2017	7:51:12	13:03:56	15:41:17	20:30:09
	MOH. MUTHOHIR	Wednesday 21 June 2017	7:58:52	12:56:02	15:48:20	20:33:55
	HARIS IHSANIL HUDA	Tuesday 20 June 2017	7:58:16	13:07:56	15:53:12	20:38:57
	TEGUH SETIADI	Tuesday 20 June 2017	7:30:16	13:02:27	15:45:31	20:45:27
	MUNIFAH	Tuesday 20 June 2017	7:58:20	12:55:17	15:48:55	20:33:13
	LAKSAMANA RAJENDRA HAIDAR	Tuesday 20 June 2017	8:07:42			21:03:29
	MOH. MUTHOHIR	Monday 19 June 2017	7:56:29	12:20:25	15:59:30	20:32:25
	MIFTAHURROHMAN	Monday 19 June 2017	7:55:59			
	LAKSAMANA RAJENDRA HAIDAR	Monday 19 June 2017	7:26:17		16:02:24	
	BOBI	Saturday 17 June 2017	7:45:03	13:05:15		
	TEGUH SETIADI	Saturday 17 June 2017	7:35:26	12:37:08		
	TEGUH SETIADI	Friday 16 June 2017	7:10:02	13:01:26	15:31:25	20:49:06
	BAGUS SUDIRMAN	Friday 16 June 2017	7:28:54	12:49:10	15:55:45	20:30:25
	MOH. MUTHOHIR	Friday 16 June 2017	7:26:52	11:42:02	15:59:03	20:32:15
	BAGUS INDRAMAN WICAKSON	Friday 16 June 2017	7:25:29			
	MIFTAHURROHMAN	Friday 16 June 2017	7:30:43			20:27:06
	EKO SISWANTO	Thursday 15 June 2017	7:57:16	13:23:54	15:31:53	21:22:31
	TEGUH SETIADI	Thursday 15 June 2017	7:00:29	13:05:41	15:42:31	21:03:15
	LAKSAMANA RAJENDRA HAIDAR	Thursday 15 June 2017	7:34:55	12:53:16	15:07:51	20:51:14

Figure 6 Verification using Minutiae Method

Testing of attendance application is done with some data trial scenario which is collection of fingerprint data that appear on the device, the fingerprint data is tested with minutiae. The results presented by the application either using the method of diagnosis is done significantly by calculating the accuracy of the symptoms entered by the user with the prosecution of human fingerprint matching. After 90 experiments conducted 30 times FVC 2002 experiments, 30 times FVC 2004 trial and 60 times 30 times BERC experiments then obtained the accuracy of image processing finger print.

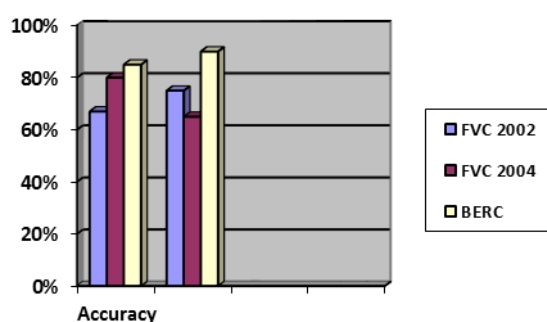


Figure 7 Result of Process taken Finger print

5. CONCLUSION

The conclusion of this journal is, the design of encryption and decryption system using biometrics system. This paper proposes a partial fingerprint matching method incorporating new RSFs with minutiae. These RSFs were defined on ridge segments where concave or convex edges are observed, and are available in conventional 500 dpi images. The RSFs can be extracted from any ridges in fingerprint images. Thus, ridge information is extensively incorporated in the partial fingerprint matching without the need to store the entire fingerprint image (texture) as a template. In addition, compared to other approaches based on entire ridge contour or image (texture), our approach is believed to be more appropriate for securing fingerprint templates and saving memory space. The proposed ridge features are represented as conventional minutia features, which facilitates a simple matching process based on the ridge features and minutiae. The reading of unique biometrics system hardware for each person produces a unique key. This key will be converted in such a way that it generates a key to encrypt plaintext into ciphertext. For the decryption process as well, the unique key obtained from reading the biometrics system is used as the key for ciphertext decryption to plaintext. And using fingerprints can provide solutions to protect and protect critical data and information. BERC is the good device to take finger print and make accuracy and precision well

DAFTAR PUSTAKA

- [1] **Nugroho, E. 2008.** Biometrika Mengenal Sistem Identifikasi Masa Depan. Yogyakarta: Andi.
- [2] **Sunyoto, Andi. 2007.** Pemrograman Database dengan Visual Basic dan Microsoft SQL. Yogyakarta: Andi
- [3] **Naslim Lathif, Achmad Hidayatno, R. Rizal Isnanto. 2001.** Aplikasi Sidik Jari Untuk Sistem Presensi Menggunakan Magic Secure 2500.
- [4] Sunardi, Nanang. **2008.** Skripsi *Perancangan Sistem Informasi Data Absensi Menggunakan FingerPrint di SMA Negeri 1 Padang.*
- [5] **Suprihatin, Andi Nurhantara. 2011.** Sistem Informasi Presensi Menggunakan Sisik Jari (Study Kasus Presensi Perkuliahan Program Studi Sistem Informasi FMIPA UAD)
- [6] **Suryadi H. S., Bunawan. 1996.** *Pengantar Perancangan Sistem Informasi.* Jakarta :Gunadarma.
- Universitas Putera Batam. 2007.** *Jurnal Analisis dan Perancangan Sistem Informasi Akademik.*
- [7] **William S. Davis,** *System Analys and DesignA Structured Approach.* (Massachusetts :Addison-Wesley, 1983), Chapter 2
- [8] **Zhao, F., & Tang, X. (2007).** Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction. *Pattern Recognition*, 40(4), 1270–1281
- [9] **Zanganeh, O., Srinivasan, B., & Bhattacharjee, N. (2015).** Partial fingerprint matching through region-based similarity. *2014 International Conference on Digital Image Computing: Techniques and Applications, DICTA 2014.*