Jurnal Mantik
Volume 3 Number 3, November 2019, pp. 151-156 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Digital File Identification Method Using Efficient Anonymous Fingerprinting

Agustina Simangungsong

STMIK Pelita Nusantara Medan. Jln. Iskandar Muda No. 1, 20154, Indonesia

Email: agustina.simangunsong@gmail.com

ARTICLE INFO

Article history:
Received: 17 Oct 2019
Revised: 24 Oct 2019
Accepted: 1 Nov 2019

***Keywords**:*
Fingerprinting, detection of identity, anonymous method of fingerprinting

ABSTRACT

Fingerprinting method is one important class of engineering protection of intellectual property in digital form. This method is a cryptographic method that is applied to detect people to redistribute an item of data by allowing a merchant (merchant) to track a duplicate to be able to note the original purchaser. Buyers dishonest redistribute illegally item of data called a traitor (traitor). Information referred to as fingerprint identification, attached to the duplication of the original item data. For the development of an application it is necessary to illustrate the application of anonymous fingerprinting methods in the detection of identity of the file redistributed. Other than that, the software also provides a tutorial to assist understanding of the working procedures of anonymous fingerprinting method. The results of the tutorial section can also be saved into a text file.

1. Introduction

Protection of intellectual property in digital form has been the subject of research in recent years have caused the emergence of various cryptographic techniques. Fingerprinting method is one important class of these techniques. This method is a cryptographic method that is applied to detect people who duplicate and distribute a digital file that is bought by allowing a merchant (merchant) to track a duplicate to be able to note the original purchaser. Buyers dishonest redistribute illegally item of data called a traitor (traitor). Information referred to as fingerprint identification, attached to the duplication of the original item data. For example, such a software development company that sells softwareaccounting that he built to the company.

Anonymous fingerprinting method first introduced by Domingo, where the method can identify the parties who redistribute (redistributors) without the help of the registration (registration authority). However, these methods require an average of N / 2 exponential operation when the merchant identify redistributors, where N is the number of the public key in the directory. To overcome these problems, Yong Li, Bo Yang and Xiang Hua propose an efficient method of anonymous fingerprinting and writing published on May 13, 2002 at Informatica 26. The proposed algorithm requires only one operation exponentially when one identify redistributors, which will increase the efficiency of the method. In addition to,

2. Theoretical Basis

A. Efficient methods AnonymousFingerprinting

Efficient anonymous fingerprinting method is a cryptographic method that can be used to detect people who redistribute an item of data by allowing a merchant (merchant) to track a duplicate to be able to note the original purchaser. Buyers dishonest redistribute illegally item of data called a traitor (traitor). Information referred to as fingerprint identification, attached to the duplication of the original item data. Efficient anonymous fingerprinting method will produce a series of figures based on the data item purchases and rows of numbers is referred to as a fingerprint.

The workings of efficient anonymous fingerprinting method can be described as follows:

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 3, November 2019, pp. 151-156 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Suppose p is a large prime number such that q = (p - 1) / 2 is also a prime number. Think of Zp * is the multiplicative group modulo p and assume g is a generator of Zp * such that calculates the discrete logarithm to the base g is difficult. Assume that the buyer B and a registration authority (registration authority) RC has a pair of public key / private key ElGamal. The private key and the xB buyer is public key is yB = gxB mod p. RC registration authority is a Trusted Third Party (TTP) and use the private key to create a certificate that can be verified by using the public key. All public key is assumed to be known and certified. The working process of the registration protocol will begin following a request from the buyer.

The working process of this protocol can be divided into several stages as follows:

1. Registration Protocol
   a. RC selecting a secret random number xr∈ Zp and send yr = GXR mod p to B.
   b. B selecting a secret random numbers s1 and s2 on Zp, such that s1.s2 = xB∈Zp and compute S1 = yrs1 mod p and y1 = GS1 mod p, s2 encrypt using public key PKR registration authority be EpkR (s2) and transmit S1, y1 and EpkR (s2) to the RC. Buyer B convince RC with zero-knowledge regarding the ownership of s1. On fingerprinting, y1 acts as a pseudonym and anonymous public key of the buyer B.
   c. RC decrypt decryption authority EpkR value (s2) using a private key SKR and check whether S1s2 mod p = yBx1 valid or not. If the verification is successful, RC returns the certification Cert (y1) and Cert (y1 || s2) to B.

   Through the registration procedure above for several times, a buyer can obtain several pseudonyms y1.
2. Fingerprinting protocol
   a. Buyer B sent [y1, Cert (y1)] and text to the merchant M, where the text is a string that identifies a purchase (purchase record). B calculates a signature ElGamal sig in the text by using a private key s1, sig is not sent to M.
      Signature process is as follows:
      - Choose a random number k ∈ Zp *.
      - Calculate the value of r and s by using a digital signature algorithm El Gamal.
      - *Signature* sig = (text, r, s)
   b. M verifies the certificate on y1 and save [y1 || Cert (y1)].
   c. B and M to compute the two parties. Input of M is text, y1 and items, where the item is genuine information that will be made of his fingerprint. Input of B is sig, s2 and Cert (y1 || s2).
      The calculations were carried out as follows:
      - ver1 = Verify1 (text, sig, y1). Signature sig on text verified using public key y1. Output of ver1 is a Boolean variable that can be considered by the merchant M as true, if and only if a successful signature verification. This verification process to ensure that the digital signature contained a record purchase is valid.
      - ver2 = Verify2 (y1, Cert (y1 || s2), s2). First, the certificate Cert (y1 || s2) verified. Second, verify that the value of the certificate Cert y1 (y1 || s2) is equal to the value y1 that are input by M. Third, check that the value of s2 on the certificate Cert (y1 || s2) is the same value as the value s2 the input by B. Output of ver2 is a Boolean variable considered by traders M as true, if and only if all the checks mentioned above all succeed. This verification process to ensure that the attached certificate is valid.
      - item = Fing (item, emb). A classic fingerprinting algorithm used to embed emb on the original information item, wherein:

        emb = text || sig || y1 || s2 || Cert (y1 || s2) ..... (persamaan.1)

      Fingerprint information obtained item and can only be viewed by buyers B. While emb an abbreviation of the embedded meaning embed or attach.
      In computing the two parties above, M gain output in advance and only if ver1 and ver2 both are true, then B can get the output in the form of items, if not, then B will not receive anything.
3. Protocol Identification
   At the time of finding a duplication redistribution (redistributed copy), M extract emb. Information extracted consists of the value specified in persamaan.1 and combined by M with proof of purchase (purchase record) [y1, Cert (y1)] to construct a proof of redistribution:
   a. *Signaturesig* the text is verified by using y1.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 3, November 2019, pp. 151-156 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

b. Checking the carry value is equal to the value y1 y1 on the certificate Cert (y1) and Cert (y1 || s2). Because the value of y1 is part of the certificate, then y1 is not possible to add your own (falsified).
c. Lastly, to identify a buyer, the merchant M calculate y1s2 = yB mod p. B dishonest buyer will be identified. It should be noted that, since s2 is certified, then the value can not be forged by the merchant M for accusing a buyer.

4. Protocol Disputation

This protocol is only performed if the merchant M showed evidence of redistribution to a judge. Traders submitting evidence (purchase records [y1, Cert (y1)] and the information extracted emb) to the judges. Judge to verify the evidence. First, she verifies the certificate Cert (y1) using the public key registration authority, then check whether y1s2 mod p = yB valid or not. If the verification process on a third protocol above all valid identification, then the owner of the public key yB will be sued. If proof of registration is required to prove that the buyer is guilty, then the judge may ask for proof of registration to the registration authority.

3. Discussion

A. Efficient Implementation Method Anonymous Fingerprinting on the Identity Tracking Digital Files

Efficient Anonymous Fingerprinting method can be used to carry out checks on the identity of the owner of the file is duplicated. In order to better understand the working process of the scenario this fingerprinting method, it is provided an example of the following case, suppose a trader wants to sell digital products on the internet. These traders want to track whether there are redistributing the digital product.

The trick is that merchants require that all buyers who want to buy their products enlisted in the service fingerprint (Traders can also develop their own fingerprint services). After that, the buyer can show the data provided by the service fingerprint. Traders will process and produce a fingerprint for that buyer. Here it is assumed that if the buyer wants to buy some digital product merchants, the buyers only need to register once.

In this study, it is not discussed on how to detect duplicate files, but the research emphasis on how to detect the identity of the buyer of the files are duplicated. Therefore, taken the assumption that traders have gained some duplication of digital files.

B. Process Analysis

Anonymous fingerprinting method to be applied to this software has several stages of the process can be detailed as follows:

1) Registration protocol

This protocol serves to register the buyer data. This protocol is carried out between the registration authority (R) and the buyer (B). Through the registration procedure for several times, a buyer can obtain several pseudonyms (y1). Figure 1 below illustrates the working process of the registration protocol:

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 3, November 2019, pp. 151-156 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

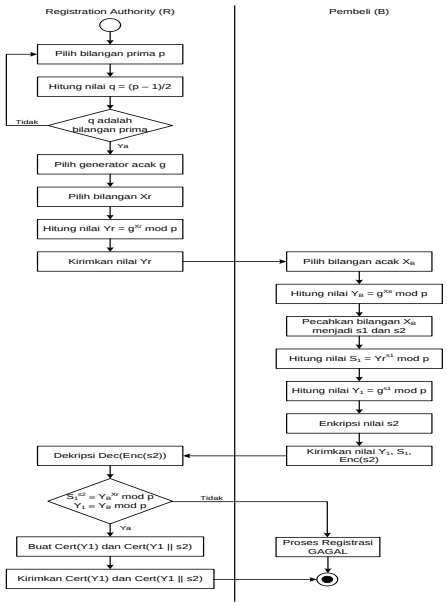

Figure 1. Registration Protocol

2) Fingerprinting protocol

This protocol is used to make a fingerprinting with buyers based on the data input and data messages. This protocol is carried out between the buyer (B) and the merchant (M). Figure 3.2 below illustrates the working process of fingerprinting protocol:

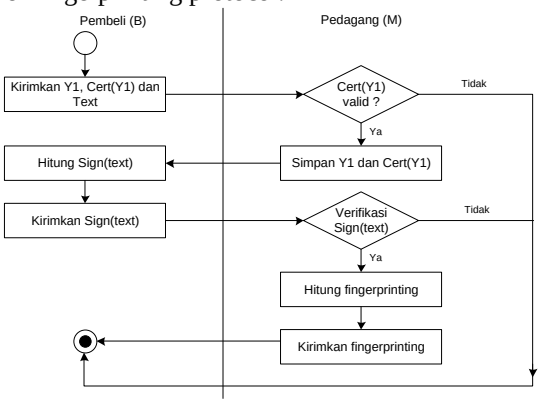

Figure 2. Protocol Fingerprinting

3) protocol Identification

This protocol serves to check the identity of a fingerprinting. This protocol is only done by the merchant (M) itself. This protocol is only done in case of redistribution carried out by buyers and traders is to track who is doing the redistribution. Figure 3.3 below illustrates the working process of the protocol:

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 3, November 2019, pp. 151-156 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

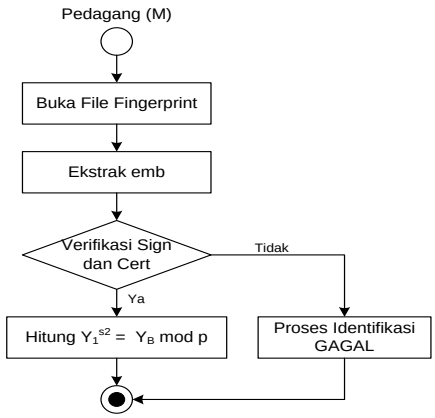

Figure 3. Identification Protocol

4) protocol Disputation

This protocol serves to provide the evidence that would be used to sue a buyer who redistribution. This protocol is done by the merchant (M) and interpreter middle / judges (J). This protocol is only done in case of redistribution carried out by buyers and traders sued buyers making such redistribution. Figure 3.4 below illustrates the working process of the protocol Disputation:

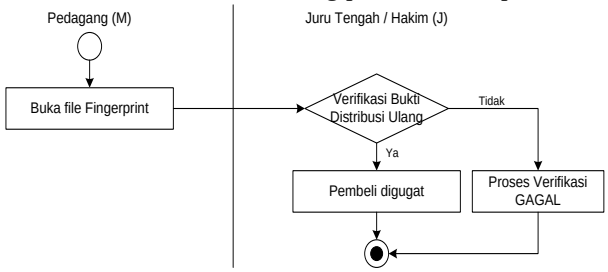

Figure 4. Protocol Disputation

C. Requirements Analysis

Analysis of the requirements of the system will be designed to include a functional analysis that describes the functionality that must be met by the software and analysis that describes the non-functional non-functional requirements related to the quality of the system.

As for some of the functional requirements that must be met by the software are as follows:

1. Functions discussed in the software include:
   a. Registration functions, which serve to generate the key data to be used in the process of fingerprinting. Numbers needed in this function can be generated randomly by computer or manually entered by the user and then verified by the computer in accordance with the provisions of the algorithm.
   b. Fingerprinting function, which serves to make a fingerprint of the data to the invoice number and code of goods purchased based on the key data generated at the registration function. Data transfer receipt (text) that is required in this function can be typed manually in the area were charging textbox.
   c. Identification function, which serves to identify the fingerprint is entered and key data generated at the registration function. Data can be entered fingerprinting required by opening a file previously saved on a fingerprinting function. Especially for comprehension section, the input of this function does not need to be entered again. The necessary data will be retrieved from the registration and fingerprinting function that has been done before.
   d. Disputation function, which serves to deal with disputes between merchants and buyers. The necessary data can be entered by opening files that have been stored previously. As for the understanding, the data input will be taken automatically by the computer of the functions previously.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 3, November 2019, pp. 151-156 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

4. Conclusion

Upon completion of this study concluded THAT detection process birthday party duplicating files can only be done with the requirement that traders must obtain the re-duplicated file and the file has been modified isinya.Laporan the results of the calculation process can be used to aid understanding of the working procedures of the method efficient Anonymous Fingerprinting. The software can only be used to aid understanding of the working procedures of Efficient Anonymous Fingerprinting method when the user has to understand all the symbols used in the method and understand the basic concepts of mathematical cryptography.

5. Reference

[1]. Kurniawan, J., 2004, Kriptografi :Keamanan *Internet* dan Jaringan Komunikasi, Penerbit Informatika Bandung, Indonesia.
[2]. Munir, R., 2006, Kriptografi, Informatika Bandung, Indonesia.
[3]. Pressman, R.S., 2002, Rekayasa Perangkat Lunak : Pendekatan Praktisi (Buku Satu), Mc Graw-Hill Companies, Inc, Penerbit ANDI, Indonesia.
[4]. Schneier, B., 1996, *Applied Crytography : Protocols, Algorithm, and Source Code in C, Second Edition*, John Willey and Sons Inc, Amerika Serikat.
[5]. Stallings, W., 1999, *Cryptography and Network Security : Principle and Practice*, *Second Edition*, Prentice Hall, Amerika Serikat.
[6]. Yong L., B. Yang and X. Hua, 2002, *An Efficient Anonymous Fingerprinting Scheme*, China.
[7]. P. Informatika, B. Darma, H. D. Hutahaean, C. Digital, C. Streching, and L. Teori, "TEKNIK PENAJAMAN CITRA DIGITAL DENGAN MENGGUNAKAN Diterbitkan Oleh : STMIK Budi Darma Medan Diterbitkan Oleh : STMIK Budi Darma Medan," vol. III, pp. 35–44, 2013.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.