An Overview of Fingerprint Template Protection Approaches

by Apri Siswanto

Submission date: 28-Aug-2017 05:21PM (UTC+0800)
Submission ID: 840513731
File name: of_Fingerprint_Template_Protection_SchemesEdited1_TURNITIN.docx (91.45K)
Word count: 4184
Character count: 25061

An Overview of Fingerprint Template Protection Approaches

Abstract— **There are two attacks that are often a serious concern by researchers and developers in biometric fingerprint systems, ie attacks in communication lines and attacks on templates stored in the database. This attack can lead to leakage of"biometric template information, thus posing a serious privacy security threat. Most fingerprint template protection techniques that have been developed fail to meet all the desired requirements of a practical biometric system such as diversity, revocability, security, and performance. This paper aims to review the various fingerprint template protection approaches (ftp) that have been proposed by researchers in recent decades. Some of the proposed schemes are standard encryption, biometric cryptosystem, feature transformation, hybrid scheme and homomorphic encryption."**

Keywords—biometric system; fingerprint template protection; security, diversity, revocability

I. INTRODUCTION

Biometric templates offer a reliable approach to user authentication issues in identity recognition systems. A wide range of biometric technologies are developed effectively that include fingerprint, iris, face, iris, palms, signature and hand geometry. Fingerprints are the most popular as they are easily captured, as well as low cost sensors and algorithms. The main purpose of using fingerprint biometric systems is to provide good authentication and can not be rejected. Authentication implies that only authorized users be able to access logical or physical resources protected by fingerprint systems and impostors are prohibited from accessing protected resources. From the user's perspective, There are two main requirements for a fingerprint biometric system to be met. Firstly, a legitimate user must have fast and precise access, then reliable to a protected service or resource. Secondly, biometric systems and personal data stored therein should be used only for predetermined functionality, that is controlling access to certain resources or services and not for other unintentional purposes.[1]

However, adversary attacks can make the biometric system not functioning properly according to the above requirements. To overcome and protect the biometric template information both in the process of registration/enrollment and authentication in the stored database, some techniques have been proposed by the researchers include standard encryption, biometric cryptosystem, template transformation, hybrid method and homomorphic encryption. This paper aims to summarize and present information on various fingerprint template protection techniques. The technique used is systematic literature review. The paper is organized in the following way. Section 2 of the paper discusses the attack on fingerprint template. Then, Section 3 presents desirable properties of fingerprint template protection. After that, Section 4 discusses fingerprint template protection approaches and Finally, Section 5 concludes the paper.

II. ATTACK ON FINGERPRINT TEMPLATE

The security guaranteed by the biometric fingerprint system can be compromised, so it is necessary to analyze the fingerprint biometrics system for vulnerability assessment in determining the extent to which intruders can compromise security on fingerprint biometric systems. Many attacks apply to any information in fingerprint biometrics systems, either attacks that use fake biometric fingerprints or unique template modifications to fingerprint biometrics systems. As identified by Ratha, et al. [2] Fingerprint recognition system is vulnerable to several types of attacks, as for the number of attack points on the fingerprint recognition system are as follows:

1. Attack at the sensor, in this attack usually the intruder using fake biometric samples can be presented in the sensor to gain access to the system.
2. Replay Attack, There is a possibility of the adversary to interpret or obtain a digital copy of a stored biometric sample and replay this signal that passes through the biometric sensor.
3. Trojan horse attacks, on this attack extractor feature can be changed with programs that generate a set of desired features
4. Spoofing the features, The biometric template generated from the vector feature are replaced by a set of synthetic (fake) features created
5. Attack on templates, the templates generated during the user enrollment can be stored locally or in network location that modify the saved template or replace it with a new template.
6. Attack on templates, In this attack, template generated during user enrollment can be stored locally or in network location. Templates stored in the database can be modified or replaced new templates.
7. Attacks on communication channels, Data sent through computer networks may be intercepted, for criminal purposes. This data can be modified, then put back into the system
8. Attack on the decision module, On this attack the trojan horse data program can change the final decision result of the fingerprint biometric system

Biometric matching is usually one part of a larger information management and security system. Thus non-biometric modules throughout the system may also experience some security flaws. There are several techniques to disrupt attacks at various points. For example, sensing a finger conductivity

or pulse can stop a simple attack on the sensor. Encrypted communication channel [2] can eliminate at least remote attack on synthesized feature factor and override final decision. The simplest way to stop attacks at override matcher, attacking the channel and modify template in database is to have the matcher and database reside in a secure location. Storing data templates in a smartcard that a user leads with them to the aplication service can eliminate some attacks of type stored template [3].

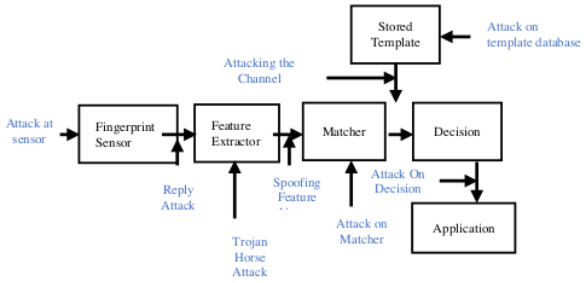

Fig. 1 Possible attack in fingerprint template protection

III. DESIRABLE PROPERTIES OF FINGERPRINT TEMPLATE PROTECTION (FTP)

There are three ways to assess the performance of fingerprint template protection, ie rotation, operational and technical. Performance protection includes the irreversibility and diversity of biometric information. Operational performance can be evaluated with the independence of modality, interoperability, and Quality of Performance. Technical performance can be evaluated with accuracy, throughput, storage requirements [4].There are four major requirement when a biometric template protection algorithm is design [5] :

2

A. Security: It should be extremely difficult to generate the original fingerprint feature set from the protected fingerprint templates.
B. Diversity: The cross-matching of a secured fingerprint templates should be ensured in such a manner that the privacy of the true owner of the template should be ensured.
C. Revocability: When the biometric template is compromised, it should be possible to revoke the compromised template and reissue a new template based on the fingerprint biometric properties .
D. Performance: The biometric template protection techniques developed should not decrease the accuracy of the recognition system.

IV. FINGERPRINT TEMPLATE PROTECTION (FTP) APPROACHES

The major fingerprint template protection schemes can be categorized into standard encryption, biometrics cryptosystem, template transformation, hybrid methods, and"homomorphic encryption such as shown in Figure 2. Each of schemes will discussed detail in the following sections.

A. Standard Encryption

To secure fingerprint templates, the widely used methodology in commercial biometric fingerprint systems is to encrypt them using standard cryptographic techniques such as RSA, DES and AES. Nevertheless, the problem is that multiple acquisitions with the same biometric properties do not produce the same feature set. Typically, the standard encryption function does not smooth the functionality and a small difference in the value of the feature set extracted from the raw fingerprint biometric data will result in large differences in the resulting encrypted features. Consequently, user cannot perform biometric fingerprint matching in encrypted domains directly, so to match query features, fingerprint templates must be decrypted. Thus, there will be a problem that is the original biometric feature exposed on every authentication attempt, regardless of whether the authentication is ultimately successful or not. Therefore, secure encryption solutions are revoked only in ideal conditions when keys are kept confidential and matched in a trusted location. If key management issues or vulnerabilities to template theft during matching are taken into account, standard encryption techniques are not good enough to secure biometric templates.[5, 6].

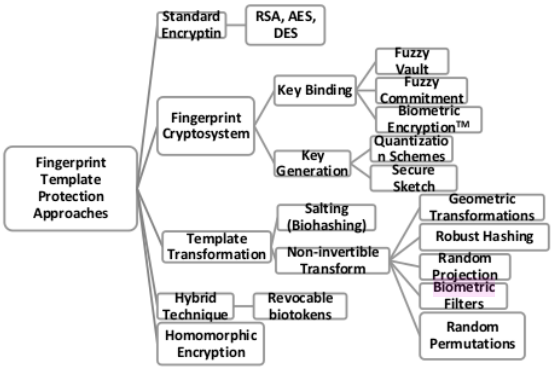

Fig. 2 A hierarchical taxonomy of FTP

B. Fingerprint Cryptosystem

In the fingerprint cryptosystems data information about the fingerprint template, usually called helper data, and stored in the database [7]. The helper data does not show important information about the original fingerprint template but is needed when matching the cryptographic key of the query fingerprint feature. Matching is done indirectly by verifying the truth of the extracted key. Error correction coding techniques are usually used to handle intra-user variations. Fingerprint cryptosystems offer high security but, not designed to provide diversity and revocability. Fingerprint cryptosystem are grouped into key binding and key generation systems based on how the helper data derived[5].Some of the techniques in this category are fuzzy vault, biometric encryption and fuzzy commitments.

Soetar, et al. [8] was the first researcher to introduce biometric cryptosystems based on key bindings. The design is

known as BiometricEncryptionTM (mytec2) which is the full version of mytec1 [9]. This encryption has deficiencies in terms of mismatch between accuracy and security. Then, the next key bindings are fuzzy vault, fuzzy vault is designed to work with biometric features that are described as minutiae in fingerprints. The advantage of this scheme is the ability to control the amount of security afforded in biometric protected templates by increasing the number of chaff points and as a result the attacker will have difficulty in polynomial reconstruction problems. Although this scheme is widely used and developed in various fingerprint security applications, several analyzes show the weaknesses of this scheme. For example Chang, et al. [10] made observations to distinguish the small points from the chaff point that attacked the fuzzy vault based on fingerprints. Since the chaff points are made one by one, they are then tended to reveal a smaller, experimentally verifiable smaller area around, the security of a fuzzy vault relying heavily on the methodology for generating a chaff point.

Scheirer and Boult [10] also discussed the vulnerability of fuzzy vaults to three potential attacks, namely, surreptitious key-inversion (SKI) attacks, blended substitution attacks and attacks via record multiplicity (ARM). The authors suggest that a fuzzy vault is particularly vulnerable to ARM attacks, where access to two or more fuzzy vaults generated from the same biometric data, but with different keys and chaff points, would enable an adversary to easily identify the original points in the two vault and thus decode the vault.

Therefore the fuzzy vault approach does not provide diversity and revocation. Then it can be concluded that if it can be compromised. the fuzzy vault vulnerability to ARM attacks allows cross-matching of templates on different systems, so user privacy can not guarantee be secured [11]. In a stolen inversion-key attack, if an attacker can recover a secret key embedded in fuzzy vault, a secret polynomial can be reconstructed directly; Thus, unprotected biometric templates can be easily separated from the chaff point. Mixed substitution attacks are very easy if the enemy is able to modify the existing fuzzy vault. In this attack, a fraudster takes advantage of the many chaff points present in a fuzzy vault to replace some of these random points with his own biometric data, in which case legitimate users and imitators can be identified using the same fuzzy vault. This is evidenced in the research of Kholmatov and Yanikoglu [12] and Scheirer and Boult [10] which presents experimental confirming the fuzzy vault vulnerability to note the multiplicity correlation attack.

Nandakumar, et al. [11] further mention the possibility of exploiting the non-uniform nature of biometric features to launch an attack on a fuzzy vault based on statistical analysis of points in the vault. The authors also note the vulnerability of a fuzzy vault to attacks during the authentication phase, where a genuine user's original template is temporarily exposed and therefore vulnerable to snooping [13].

The second key binding is the fuzzy commitment, which was first created by juel and watenberg [14]. According to Simoens [4], et al. Fuzzy commitment is a biometric cryptosystem that can be used to secure the biometric properties shown in binary vector form. The fuzzy commitment scheme characteristic is useful for biometric authentication system applications, where data is subject to random noise. Because the scheme is fault tolerant, it is able to protect biometric data such as conventional cryptographic techniques, such as hash functions, used to protect alphanumeric passwords [15].

3 Generally, in the key generation fingerprint cryptosystem, helper data is generated only from the fingerprint template while the cryptographic key is generated directly from the helper data and query fingerprint feature. The key generation of direct biometrics is an attractive template-protection approach that can be very useful in today's cryptographic applications. However, it is difficult to generate keys that can fund stability and high entropy due to intra-user variation in templates. It is difficult to develop a scheme that generates the same key for different templates from the same person and at the same time has a very different key for different people. Examples of this scheme are: secure sketch and quantization schemes.

In the quantization scheme method, helper data is quantized to obtain a stable key. This scheme takes feature vectors from multiple biometric samples and gets feature element intervals. The interval is encoded and the stored in helper data. Throughout authentication, biometric features are calculated and mapped to determined intervals. Several studies in this method such as [16] use the Divide and Conquer method for fingerprint images, and bio keys are generate using minutia set. Yang, et al. [17] proposed a fingerprint cryptosystem by modifying Voronoi Neighbor Structure (VNS). In the same year, Yang, et al. [18] developed fingerprint authentication system that uses topological code for local enrollment and security enhancements based on Delaunay Quadrangle.

C. Fingerprint Template Transformation

In this approach, the transformation function is used to convert the user's fingerprint template listed in the system into a protected fingerprint template. This transformation function is indicated by a set of User-specific parameters, derived from random external keys or random passwords. After that, only the protected templates are stored in the system database. Matching process is done in the transformed domain. salting and non-invertibles are two of the most popular schemes in feature transformation approaches. Basic Security salting scheme exists on the secrecy of a key or a keyword. While the security of non-invertible transformation techniques using one way of computing functions is difficult to reverse, even if the key is known. However, the main disadvantage of this technique is that system security is difficult to verify. It is for this reason that no mathematical foundation is used to perform a robust security analysis. Furthermore, it is assumed that the uniform biometric feature distribution [19] and enemies may be able to utilize non-uniform biometric properties to launch attacks and require little effort to compromise system security.

- Salting

Salting is an approach used two-factor authentication scheme, in which an unprotected biometric template is transformed into a protected template via a function Specified by an external key or a user-specific keyword. Because the transformation can be reversed for the most part and will be used during authentication then the key must be kept or

remembered safely by the user. To increase the entropy of the biometric template, additional information is needed in the form of a key, making it difficult for the opponent to guess the template [5].

The limitations of the salting approach is that the security of this scheme depend on the secrecy of the key or password [13, 20]. As a result, effective key management procedures must be put into place, or else the user is obliged to memorise the secret key; however, relying on users memory for the protection of complex secret keys re-introduces the weakness of password-based schemes that we are trying to circumvent . Since matching is performed directly in the transformed domain, the salting functions must be designed such that they do not have an adverse effect on the recognition performance. This becomes especially important in the presence of large intra-user variations. Salting methods generally use quantization to deal with intra-user variability during matching in the transformed domain.

Several studies related to fingerprint salting approach will be discussed below. Teoh et al [21] introduced the bio phasor technique. This method is the pseudo-randomgnumbergmixing iteration with the fingerprintgfeature. This work is considered a stolen key scenario. Then, Jin, et al. [22] proposed salting biohashing. The biohashing procedure was initially proposed for the fingerprint modality, and it consists of two stages. Firstly, the extracted fingerprint feature vector is transformed into a translation, rotation, and scale invariant feature set, employing the Wavelet Fourier-Mellin Transform $(WFMT)^2$. Secondly, the resulting data is discretised via an inner product computation between the invariant feature vector and a tokenised pseudorandom number sequence. The second stage of this process produces the protected biometric template vector, which is referred to as a BioHash.

The Biohashing procedure has been proven to be advantageous in several ways. Firstly, biohashing simultaneously provides high intra-class variation and extremely low inter-class correlation, which essentially leads to an Equal Error Rate (EER) of zero (when the legitimate token is used). This means that the occurrence of a False Accept is eliminated without a corresponding increase in the FRR [23]. It has also been claimed that Biohashing has a high tolerance to data capture offsets, such that the same biometric trait acquired at different times will produce highly correlated bit strings (BioHashes) [22]. This is due to the invariance of the feature vector created during the first stage of the Biohashing process, as well as the subsequent discretization of the invariant feature vector in the second stage. Another advantage of Biohashing is that it addresses the problem of irrevocability of biometric features: a user's compromised BioHash can be easily revoked and replaced with a new one by using a different secret seed for enrolment.However, Biohasing schemes have weaknesses that have been presented by researchers. The most commonly analysed limitation of the Biohashing approach is the degradation in matching performance when an adversary has access to a user's secret key (seed) and uses the legitimate key with their own biometric features in order to fool the system into authenticating them [24].

Several researchers have presented methods for resolving performance degradation resulting from a stolen-token scenario, such as [25-27]. Beacuse a salting approach is by nature invertible, almost no any existing literary works focus on improving the non-invertibility property of Biohashing; however, there are two suggestions are presented in [28, 29]. In fact, Biohashing on its own technically cannot be made to be non invertible. A hybrid protection scheme, incorporating techniques other than salting, would be required; for example, applying Biohashing to a non-invertible template. Other salting techniques, which do not adopt Biohashing, are also available in the literature; such as [30, 31].

- *Non-Invertible Transform*

One-way functions applied to biometric data. To update biometric templates, function parameters must be changed. In case the transformed parameters are compromised the attacker can not reconstruct the original biometric template. Because of intra-class variations, transformations need to align biometric templates to perform effective comparisons and this leads to reduced authentication performance. A non-invertible transform shows the impossibility on obtaining the original biometric data from its transformed version. The parameters of the transformation function are specified by a key, but knowledge of the key and/or the transformed template does not facilitate recovery of the original biometric template [5, 32].

The major advantage of the non-invertible transform scheme approach compared to the salting approach, and it means that biometric templates that are protected using non-invertible transforms are generally more secure than those protected using the salting approach. Then, a related advantage of the non-invertible transform approach is that, unlike salting, it does not require storage of any secret information. The next positive aspect of non-invertible transforms is that they tend to leave the protected biometric template in the same feature space s its unprotected counterpart. In this case, intra-user variations in the transformed biometric templates can be robustly handled by using existing, sophisticated matchers, thereby reducing the error rates of the biometric system [33]. Furthermore, the matching scores obtained are proportional to those obtained in the original space, and thus can be used in the design of a secure multibiometric system through a scoreline-level fusion method.

The main limitation of the non-invertible transformation method lies in the difficulty of designing a good one-way function. The transformation function must ensure that the biometric features from the same user maintain a high similarity in the transformed space, while features from different users are completely unrelated after transformation. However, the transformation must also be non-invertible, so that an adversary is unable to collect any information about the original biometric template from its protected counterpart. There is a trade-off between discriminability and non-invertibility, since it is challenging to design transform functions that satisfy both requirements simultaneously.

Consequently, often the greater the amount of distortion applied to the original biometric data by the transformation, the worse the recognition performance among the protected biometric templates. This means that the non-invertible

transform approach typically suffers from a security versus performance trade-off. Furthermore, the transformation function relies heavily on biometric features to be used in specific applications. This analysis makes evident a clear comparison between the salting and non-invertible transform approaches. While salting schemes (such as BioHashing) generally tend to either preserve or improve the recognition performance of the biometric system into which they are incorporated, non-invertible transforms often have the effect of degrading the recognition accuracy somewhat. On the other hand, non-invertible transforms tend to impart more security to the protected biometric templates compared to salting approaches, which are invertible with the revelation of the user-specific key.

In this scheme,the most influential researcher are Ratha, et al. [34]. They proposed and analyzed cancelable biometrics fingerprint using non-invertible transforms for generating cancelable fingerprint templates. It can change the raw biometric templates by using either feature or signal domain transformations. The three transformation functions are Cartesian transformation, polar transformation and functional transformation. Research with the same technique is also done by Yang, et al. [35] which developed fingerprint template protection with non-invertible transformation by considering local and global features of minutia pointss. The distance between the minutia pair is projected vertically to the circle.. Later, Lee and Kim [36] Proposed a fingerprint image is represented into minutiae points and created using string bits. Minutia points of the fingerprint image are mapped to a 3D array that is divided into small cells. A string of bits is generated by finding which cells include minutiae points. Subsequent research conducted by Zhe and Jin [37], they proposed the protection of a fingerprint template obtained using a projected MVD feature at random. Ahmad, et al. [38] introduced a pair of polar relationships of minutiae. The correlation-based filter method using chip matching was proposed by Takahashi and Hirata [39]. Wang and Hu [40] proposed the Densely Infinite To One Mapping (DITOM) approach use of Correlation Invariant Random Filtering (CIRF). Das, et al. [41] meant a method based on the Minimum Distance graph. The hashing algorithm is constructed using this graph and an appropriate search algorithm is used to match the resulting hash. Ferrara, et al. [42] making the non-invertible Cylinder Minutiae Code (pMCC) for fingerprints as a fingerprint enhancement enhancement fingerprint.

D. Hybrid Methods

Several fingerprint template protection schemes used combination of feature transformation and fingerprint cryptosystems. Usually it called hybrid methods. Several hybrid system examples are presented in the literature, some of which even incorporate traditional cryptographic hashing functions into the hybrid protection system. For Example hardening a fingerprint based fuzzy vault with a user-specific password, combined key binding with salting [11]. An application-specific key release scheme that retrieves a cryptographic key bound to a BioHashed fingerprint, combined salting with key binding methods [43].

In addition, Several studies that have been done in fingerprint template protection based on hybrid scheme such as Boult, et al. [44], Feng, et al. [45], Nagar, et al. [28]. Furthermore, Chin, et al. [46] proposed a hybrid system using fingerprint and palmprint features, then Sandhya and Prasad [47] constructed Delaunay triangles from fingerprint minutiae. Finally, Jin, et al. [48] proposed a long ECC free key-binding scheme with a cancelable transforms for minutia-based fingerprint biometrics. The advantage of hybrid protection schemes is that they can combine the high revocability and diversity properties characteristic of feature transformation approaches with the high security offered by fingerprint biometric cryptosystems [5].

E. Homomorphic Encryption

Another alternative, apart from the above 4 methods is homomorphic encryption. This technique allows a limited subset of calculations on encrypted data. Combining Homomorphic Encryption with a fingerprint recognition system will meet the requirements of Fingerprint Template Protection without degrading the accuracy [49]. The fingerprint template protection study under the Homomorphic Encryption scheme was developed at Rane et al. [50], for fingerprint applications, they use a Hamming distance calculation. Then, Barni, et al. [51] shows distributed biometric systems by utilizing cryptosystems, homomorphic encryption on Fingercode templates in a semi-honest model.

V. CONCLUSION AND FUTURE WORK

This paper provides and summarizes information about research issues related to fingerprint template protection. Based on a survey of 51 papers conducted it can be concluded that there are 5 techniques that can be done to solve the problem of fingerprint template protection that is encryption standard, biometric cryptosystem, template transformation, hybrid methods and homomorphic encryption. Then there has not been the best approach to fingerprint template protection that actually meets the template security requirements, revocability. Diversity and performance. Application requirements and user-desired scenarios play a key role in the selection of fingerprint template protection schemes.

An Overview of Fingerprint Template Protection Approaches

ORIGINALITY REPORT

19%	5%	18%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Mulagala Sandhya, Munaga V. N. K. Prasad. "Chapter 14 Biometric Template Protection: A Systematic Literature Review of Approaches and Modalities", Springer Nature, 2017 Publication	6%
2	The International Library of Ethics Law and Technology, 2012. Publication	3%
3	jrbp10.unizar.es Internet Source	3%
4	Anil K. Jain. "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, 2008 Publication	2%
5	www.archive.org Internet Source	2%
6	Lecture Notes in Computer Science, 2007. Publication	1%
7	Submitted to Jawaharlal Nehru Technological University Student Paper	<1%

8	Submitted to Trust Academy Student Paper	<1 %
9	Submitted to Swinburne University of Technology Student Paper	<1 %
10	Ferhaoui Chafia, Chitroub Salim, Benhammadi Farid. "A biometric crypto-system for authentication", 2010 International Conference on Machine and Web Intelligence, 2010 Publication	<1 %
11	Madhavi Gudavalli, S. Viswanadha Raju, K. S. M. V. Kumar. "A template protection scheme for multimodal biometric system with fingerprint, palmprint, iris and retinal traits", Proceedings of the CUBE International Information Technology Conference on - CUBE '12, 2012 Publication	<1 %
12	Nagar, Abhishek, Karthik Nandakumar, Anil K. Jain, Jana Dittmann, Adnan M. Alattar, and Edward J. Delp III. "", Media Forensics and Security II, 2010. Publication	<1 %
13	Ann Cavoukian. "Biometric Encryption: The New Breed of Untraceable Biometrics", Biometrics, 10/26/2009 Publication	<1 %

14	Jin, A.T.B.. "An efficient fingerprint verification system using integrated wavelet and Fourier-Mellin invariant transform", Image and Vision Computing, 20040601 Publication	<1%
15	Marasco, Emanuela, and Bojan Cukic. "Privacy protection schemes for fingerprint recognition systems", Biometric and Surveillance Technology for Human and Activity Identification XII, 2015. Publication	<1%
16	Zhou Lingli, Lai Jianghuang. "Security algorithm of face recognition based on local binary pattern and random projection", 9th IEEE International Conference on Cognitive Informatics (ICCI'10), 2010 Publication	<1%
17	S. Sridevi Sathya Priya, P. Karthigaikumar, N. M. SivaMangai. "Chapter 47 Generation of 128-Bit Blended Key for AES Algorithm", Springer Nature, 2015 Publication	<1%

Exclude quotes	On	Exclude matches	< 5 words
Exclude bibliography	On		