IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Advanced Security Framework for Enabling Protection in Fingerprint Templates

Dr.R.G.Kumar[1] P Chandana[2] K Divya[3] B Bhargav[4] K Chandrashekar Balaji[5]

[1]Associate Professor, [2345]UG Student, Department of Computer Science and Engineering, Siddharth Institute Of Engineering & Technology, Tirupathi, Andhra Pradesh, India,

ABSTRACT:

Biometrics has arisen as an autonomous and trustworthy alternative to old technologies that relied on PINs or passwords, in which a subject's behavioural or physiological traits allow for his identification. One benefit of biometric characteristics is that they cannot be misplaced or forgotten. Although BTP technologies are used to create the biometric references for the registered subjects, it is still possible to impersonate a specific subject using a template obtained from a database without the BTP scheme realising it. The notion behind adding artificial templates to the system to thwart these attacks comes from the Honey words strategy. For the purpose of safeguarding conventional passwords when multiple password hashes are kept for each subject: the hash for hashes for the actual password as well as for imitation or honeypot words. More recently, a framework known as Honey Templates for the use of the honey words concept in biometric authentication systems was proposed, and a specific case study on face verification based on Eigen faces was applied on a small database, demonstrating its effectiveness in terms of both irreversibility and recognition performance.

Keywords: *Honey words, digital signature. Hash code for sugar words.*

INTRODUCTION

Digital images are widely employed in a wide range of applications, including the medical industry, military communication, remote sensing, etc., thanks to technological improvements. Information that is private and sensitive may be contained in these pictures. Images must therefore be secured against illegal access. In the past, a lot of image protection strategies have been put forth. Encryption is the method used most frequently to protect the photos. In this method, the plain image is converted into an encrypted image using a secret key and an encryption algorithm. The encrypted image appears chaotic and is therefore likely to catch the attacker's eye. Sensitive data may be exposed if an image is recorded and stacked. The Visually Meaningful Encrypted Image (VMEI) technology is created in this regard. which first secures the real image before concealing it in a reference image. The resulting encrypted picture resembles a regular picture. As a result, the VMEI methodology offers greater security than straightforward picture encryption methods. The necessity of person authentication has increased dramatically. Many vendors now provide corporations, organisations, and other users online information storage and transmission services. Because of its quick access times, ease of sharing, and many other benefits, it is a superior option to conventional information storage and transmission techniques. Information can be found in written documents, digital photos, audio files, and videos. Information security is crucial to protect it against damage, theft, release, disclosure, alteration, and unauthorised access, because it is a resource for any company or group. One of the types of data used to store visual information and transmit confidential

information via a computer network is a digital image. A secret image can be encoded using image encryption in a way that an unauthorised user cannot decipher. Several picture encryption techniques have been developed in recent years. The spatial and frequency domains serve as the foundation for these methods. Algorithms typically use matrix transformation to jumble the pixels in the spatial domain and eliminate the pixels' link with the hidden image. The encryption technique first converts the spatial secret image into the frequency domain, modifies the coefficients in accordance with specified requirements, and then converts the frequency domain.

LITERATURE SURVEY

Attacks using a mask and honey templates For more than 20 years, cybersecurity has used deception and decoy-based processes to identify data leaks and intrusions. Among other instances, honey pot servers give the impression of being a genuine component of a system while really being isolated and watched in an effort to entice and deter attackers [20]. Using honey files to draw hackers and catch them when they visit such files is another tactic, as is the most recent honey words method to track leaked hashed passwords. In each of such systems, the actual data (the sugar object) is concealed among the system's fake honey objects. The latter should adhere to two conditions. a) undetected: to fool an attacker, honey objects must be difficult to tell apart from sugar-words b) Confidentiality: The sugar item must be kept a secret from the honey objects.

A form of Internet-based computing known as "cloud computing" makes data and shared computing resources available on demand to computers and other devices. It is a framework for providing universal, on-demand access to a shared pool of reconfigurable computing resources (such as servers, networks, storage, applications, and services), which may be swiftly deployed and released with little administration labour. Users and businesses can store and process their data in third-party data centres that may be located far from them, anywhere from across the city to halfway around the world, thanks to cloud computing and storage options. In order to achieve coherence and scale economies, cloud computing depends on resource sharing. analogous to a utility over an electricity network, such as the grid.

Learning is the process of gaining new knowledge, behaviours, abilities, attitudes, or preferences, or of changing and reinforcing ones already held. It may involve the synthesis of several sources of information. Humans, animals, plants, and some machines are all capable of learning. Progress often follows a learning curve over time. Learning is a process that takes place over time and is impacted by prior knowledge. In light of this, learning may be seen of as an activity rather than a body of factual and procedural information. Learning causes the organism to change, and such changes are largely long-lasting.

Authentication using biometrics

Using a component of your physical characteristics to identify you is known as biometric authentication. This could be a physical trait like a fingerprint, iris or retina scan, or it could be something else. It is possible to employ a single attribute or several features. Everything is dependent on the desired level of security and the infrastructure. While using biometric authentication, the bodily trait being looked at is typically assigned to a username. After the user has been authorised, choices are made using this username. In certain circumstances, the username must be entered by the user when attempting to authenticate; in other circumstances, the username is determined by running a lookup on the biometric sample.

Using a component of your physical characteristics to identify you is known as biometric authentication. This could be a physical trait like a fingerprint, iris or retina scan, or it could be something else. It is possible to employ a single attribute or several features. Everything is dependent on the desired level of security and the infrastructure. While using biometric authentication, the bodily trait being looked at is typically assigned to a username. After the user has been authorised, choices are made using this username. In certain circumstances, the username must be entered by the user when attempting to authenticate; in other circumstances, the username is determined by running a lookup on the biometric sample.

By comparing the physical component you present for authentication against a copy that has been stored, biometric authentication is carried out. For comparison with the saved sample, you might place your finger on a fingerprint reader. The authentication is deemed successful if your fingerprint matches the one on file.

Using an encryption method to conceal data

Typically, a camera and fingerprint scanner will be used to gather biometric data on the client side, and that data will then be sent to a cloud service provider to perform complicated tasks like face and fingerprint identification. In these circumstances, the transmission of facial photos and fingerprints from the client side to a server is a significant security risk since a hacker could attempt to steal that information and then use it to take over the authentication system. In this chapter, we go over a secure method for transmitting fingerprints and face photos using an encryption strategy that uses reversible data hiding (RDH). RDH is a method for concealing some data. by employing a concealing medium in a way that makes it possible to later recover the original images along with the hidden message. To conceal the secret message in an image, an RDH via encryption strategy will combine the RDH process and the image encryption process into a single job. In this chapter, we suggest a new paradigm in which the compressed fingerprint data will be integrated into the facial image as a secret message using a reversible data hiding technique. After RDH, the encrypted image that was obtained will be sent for additional processing to the cloud service provider.

Passwords, Vulnerabilities, and Exploits

One of the most susceptible methods of user authentication is the usage of passwords. When we consider how things are used, we may observe this in action.Since users frequently use the same password on various websites, if an attacker is able to access one of their accounts, they can access all of them. Users frequently use the same password for both their online banking account and their email.

Several security concerns with passwords exist in addition to their lack of uniqueness. If a user doesn't update their password frequently, an attacker may eventually be able to crack it more easily. Also, it's typical for consumers to select weak simple words and no numbers or special characters for your passwords (such as "password" itself).
The following are some of the most frequent security concerns with password-based logins:

Forceful Assault

A brute force attack is a hacking technique that uses trial and error to attempt a huge number of password combinations in an effort to crack passwords (such as login credentials and encryption keys). It is a straightforward but effective approach that is frequently employed when an attacker only has access to limited data about the target, such as a username, or when they are aware of the basic format of the password but not its exact contents.

Consequences of attacks using forcefully

Your private information is in danger.
To destabilise a network, hackers disseminate malware.
Hackers take over selected systems and use them for bad purposes.
Such assaults might destroy the reputation of your business.
How can brute force attacks be stopped?
Employ lengthier, character-type-diverse passwords.
Often change your passwords.
For each website, use a separate username.
To automatically keep track of your internet login information, use a password manager.

Attacks by Phishers

In a phishing assault, which is a popular kind of cyberattack, hackers send bogus email messages that seem to be from a reliable source. Hackers attempt to steal sensitive data using this technique, including login credentials and credit card information. Sometimes, hackers carry out this action to install malware on the victim's device and get login credentials for employees or other information for an attack against a particular target.

Types of phishing attacks

Phishing that is misleading uses "spoofed" email addresses to make the target feel the message is coming from a trusted source. To persuade the victim that they must act right away on a matter, attackers frequently use the name of an actual person within the firm.

Spear-phishing: This sort of assault is tailored, targeting specific individuals or departments in an organisation. In order to acquire the trust of their intended victims, spear-phishers will conduct research to identify who they are trying to target and tailor their emails specifically for them by include personal information such as names, work titles, locations, and more.
Whaling: Using spear-phishing techniques, whaling targets senior staff members within an organisation. These attacks frequently take place during phone calls or video conferences. since they typically target CEOs and CTOs of a firm, rather than email.

How can phishing assaults be stopped?

Ensure the safety of all company equipment by deploying security software. Use a network access device update requirement policy.Multi-factor authentication should be used.
To reduce the security risk, carefully open and read your emails.

performance assessment

formally determining a person's work-related behaviours and their results in a certain role or environment. In financial trading, the goal is to determine if a person exceeded or fell short of market or industry norms in terms of wealth addition to the company and/or its clients. also known as performance evaluation. Biometrics with revocation This method uses a function derived from a user-specific factor, such as a random string or password, with the goal of creating a new and secure version of the original biometric template. The diversity property can be attained by employing various functions in various systems. As a result, cross-matching attack can be avoided by individuals who access numerous biometric-based authentication systems. This approach is divided into two sub-approaches, as described by Jain et al. in [2] as follows: 1) Seasoning: The term "salting strategy" refers to all methods that modify the initial biometric template by a certain invertible function. This kind of operation frequently depends on a secret element (also called an authentication key). When a template that has been altered has been compromised, the user must alter the secret factor, such as passcode-change. For this reason, this technique satisfies the cancelable condition. The outcomes of the transformation procedures also change because different users obviously select various components. As a result, this strategy's discriminating feature is a strong point. Nonetheless, the principal disadvantage is likewise brought by by that unknown element. The first reason is that we must maintain its secrecy at all costs. Second, if it is made public, attackers can discover the users' original biometric templates. Some of the biometric template protection systems suggested in [3-5] are based on the salting approach and are well-known for using a random projection technique with a normal matrix (considered as a secret factor). Because it preserves distance, this method is proven to be the most common. The typical projection method, on the other hand, necessitates complicated multiplications, which raises the cost of calculation. 2) Non-invertible transform: In this method, a function used to convert the original biometric templates is non-invertible. To put it another way, it is thought of as a one-way

function, which makes it simple to calculate the output but challenging to convert to the input. Users can now reveal the factor that was utilised to create the converted function because the key is no longer secret in this situation. Due to non-invertible, this strategy delivers stronger security than salting approach. But as security levels increase, recognition accuracy declines. Non-invertible boosts security while lowering discrimination since it raises the entropy of the modified data. It is difficult to balance discriminating on non-invertible transformation approaches.

Examples of this strategy are provided in [6, 7] for fingerprints and [8] for faces, among other places. The fuzzy vault approach in [9] has the cancelable property thanks to periodic function-based transformation. Due to the many-to-one mapping of the periodic function in this scheme, this transformation ensured the noninvertible. Nonetheless, it must be made clear whether or not this transformation satisfies the discriminatory property. Biometric Cryptosystem, B. This method encrypts biometric data using the cryptography idea. It was initially suggested to use biometric data to generate a secure key. Yet, this method is now frequently employed to preserve biometric template data. This method's advantage is that it has a higher security level than the alternative because its output is an encrypted template. Yet, the primary flaw in the biometric cryptosystem is the lack of revocability. Clearly, it is not intended for this property. Key-binding and key generation are introduced as two sub-approaches of the biometric cryptosystem approach, following Jain et al in [2]. 1) Key-binding: This technique uses users' unique biometric templates to secure the cryptographic key. A user's original biometric data and a random key are frequently inputs into this process, which subsequently outputs what is known as assistance data. When a user enters similar biometric information, helper data from the database is used to retrieve the key in the following phase. In essence, good helper data shouldn't reveal any details about either the key or the original biometric template. That improves the appearance of the security need in this method. This is why numerous academics have worked on this area and presented numerous works, including fuzzy commitment in [11], fuzzy commitment in [10], and fuzzy vault in [12–15]. It demonstrates that individuals are curious about the cryptographic key used to safeguard the biometric template. Nonetheless, every asset approach must admit that the absence of revocability property is a significant disadvantage. 2) Key generation techniques: these methods create the cryptographic key directly from the biometric template of the user. Moreover, the user of this key is confirmed. The authentication system can reissue the exact key by using key generation-based approaches if a user can supply it with similar biometric data. Hence, there is no need to raise concerns regarding the security of cryptographic keys. The approach's poor discriminability is its fundamental flaw. Designing a method that can provide a stable key while retaining the high entropy of biometric data is really difficult.

Recent Research:

Because biometric data is so sensitive, we need to safeguard the data that biometric systems manage and store to prevent biometric data leaks. Biometric template protection (BTP) technologies provide answers to privacy-preserving biometric authentication in this setting. They are frequently divided into two categories: cancellable biometrics, in which biometric samples are obscured irreversibly, and biometric cryptosystems, in which a key is either retrieved from or bound to a biometric sample. Since cryptosystems are becoming more widely used, new security measures must be added.In large-scale applications, cryptosystems add a lot of processing overhead. The use of honey words is suggested as a method of protecting conventional text passwords.

SUGGESTIVE METHODOLOGY

It is still possible to impersonate a specific subject using a template taken from a database without the BTP scheme realising it, even if biometric references for the registered subjects are built using BTP technology.

The notion behind adding artificial templates to the system to thwart these attacks comes from the Honey words strategy. We

suggest protecting bio-passwords by creating and maintaining hashes for both the actual bio-password and additional fictitious passwords or honey words for each subject. In this article, we present an universal (trait-independent) BTP method applied to Finer-print templates that satisfies the BTP scheme's requirements while also being able to recognise and defend against masquerade attacks.

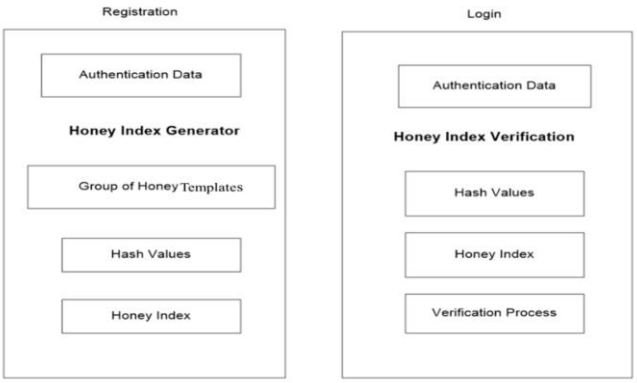
CONTRIBUTIONS

Real template for sugar is concealed among the honey templates kept in the database.

In order to trick attackers, honey templates—artificial templates inserted into each subject's file on the authentication server—are used.

Sweet templates: a collection of biometric templates that includes the subject's actual sugar template and artificial honey templates.

System that determines if a template submitted by a subject is sugar or honey is known as the template honey-checker.



In conclusion, Random Projection provides a method for dimensionality reduction that also protects biometric template privacy. Its capacity to meet the cancelability condition is a noteworthy quality. Because they preserve discriminability, transformations based on random projection are found to be the most common and commonly employed. This type of approach has numerous variations, including multi-space projections [22], random multispacer quantization, random projection with vector translation [23], etc. B. Quantization Transform Designing a cancelable template transformation technique that meets the desired criteria for cancelability and non-invertibility while maintaining the authenticity of an authentication system is a difficult task. The cancelability is provided via Random Projection; The original approach, however, does not assure the non-invertibility condition. This is the rationale behind the addition of the quantization complement step to the RP method, which renders the transform non-invertible. A surjective one-way function, Fig. 3. The surjective one-way function (shown in Fig. 3) is typically the foundation of quantization transforms that can achieve noninvertible, and its inputs are the cancelable biometric templates. The majority of these non-invertible biometric template protection techniques are not resistant to change within a class. In this circumstance, especially in binarization processes where the output of a quantization transform is a binary string, it is rather challenging to satisfy the intra-class condition. In order to complete random projection with non-invertibility, a decent quantization approach should maintain discriminability.

The outcomes of this function are converted into bit values at a specified threshold. The collection of random points P is produced at random. With two random components (threshold and point), the entropy of the final binary string is large. The thresholds for this process should be trained using the training data to ensure discriminability. Another method for giving the cancelable biometric template non-invertibility is to use a median filter. It is a non-linear digital filtering method that is frequently used to get rid of noise in images and signals. Because it can maintain edges while reducing noise, it is frequently employed in digital image processing. It is used to create the altered feature vector Z from the cancelable biometric template Y wherein the intensity levels are randomly distributed in one neighbourhood (Fig. 5). In order to identify the group representative,

the median filter takes into account each element of the input vector in turn and groups it with its neighbours.

The median of those values is applied rather than just substituting the mean of the neighbourhood values for the value of an element. It is calculated by first sorting every element in the immediate vicinity, after which the value of the middle element is chosen to take the place of the element being considered. The "window," which moves over the entire vector, is a pattern of neighbours. One-dimensional (or higher-dimensional) data, such as feature vectors, can be filtered using a median filter. In this study, we attempt to prevent the median filter from inverting a cancelable feature vector.

FUNCTIONAL MODULES

AUTHENTICATION

The process of authenticating a single piece of data (datum) or entity involves establishing the veracity of one of its attributes.

Authentication is the process of genuinely verifying a person's identity, as opposed to identification, which is the act of expressing or otherwise indicating a claim ostensibly attesting to a person's or thing's identity.

It could entail establishing the authenticity of a person's identity credentials, a website's legitimacy with a digital certificate, determining an artifact's age through carbon dating, or certifying that a product is what its packaging and labelling claim it to be.

In other words, authentication frequently entails confirming at least one form of identification's legitimacy.

HONEYPOT

A computer system on the Internet known as a "honey pot" is specifically designed to draw in and "trap" persons who try to hack into other people's computers.

A honey pot is a trap meant to detect, deflect, or in some other way prevent attempts at unauthorised use of information systems in computer language.

A computer, data, or network site that looks to be a part of a network but is actually isolated and watched over and that appears to hold information or a resource of value to attackers is considered to be a honey pot. It's comparable to when the police lure a criminal before conducting covert surveillance.

TEMPLATES FOR HONEY

The study's basic but ingenious idea is to tie each user's account with a phoney biometric template, referred to as a "honey template." When an enemy obtains the list of biometric templates, she finds numerous candidates for each account, making it impossible for him or her to determine which biometric template is authentic.

As a result, if an adversary attempts to log in using a honey biometric template, the system administrator can identify the broken biometric template files.

We make advantage of the Gen Honey template generation method ().

Keep in mind that the Gen(construction)'s directly affects the method's strength and efficacy.

HONEY TEMPLATE GENERATION METHODS AND DISCUSSIONS

We divide the techniques used to create honey biometric templates into two categories.

The legacy-UI (user interface) processes make up the first group, while the modified-UI procedures, whose template-change UI has been improved, fall under the second.

The take-a-tail approach is provided as an illustration of the second type.

This method generates a randomly chosen tail for the user to append to his or her biometric templates. The outcome is the user's new biometric templates.

AN ANALYSIS OF HONEY TEMPLATES' SECURITY

Denial-of-Service: Denial-of-service (DoS) attack is covered for the following scenario: The adversary is familiar with the Gen() technique and is able to generate every honey word that could possibly exist given a given password.

Forceful Attack:

In the previous attack, we point out that if a strict policy is executed in a honey word detection, system may be vulnerable to DoS attacks affecting the whole system.

On the other hand, a soft policy weakens the influence of honey Templates.

In this regard, we describe the following attack to demonstrate an adversary can capture an amount of accounts in case of a light policy.

In the last attack, we made the point that if a honey word detection system is subjected to a rigorous policy, the system may be vulnerable to DoS attacks that take the entire system down.

A soft policy, on the other hand, lessens the impact of honey Templates.

In this context, we explain the ensuing attack to show that, even with a lax policy, an opponent can seize a sizable number of accounts.

HONEYCHECKER

The mechanism of the honey template is as follows: The honey biometric-templates generating algorithm Gen creates a list Wi for each user ui (k).

The biometric-template list Wi = (wi;1;wi;2;wi;k) and ci, where ci is the index of the correct biometric-templates, are both output by this procedure, which takes input k as the number of delicious biometric-templates (sugar biometric-templates).

The main server's database contains the username and the hashes of the sweet template as ui (vi;1; vi:2;::: ; vi;k) > tuple, whereas ci is kept on a different server known as the honey checker.

It is more difficult to compromise the system as a whole by keeping template hashes on one server and ci in the honey checker, so providing a fundamental kind of dispersed security.

Algorithm

1. ***Procedure Bloom algorithm(L)***
2. *w ←random(L)*
3. *d ←length(w)*
4. *Honey Template(1)←w(1)*
5. ***For j←2 to d do***
6. *W ←random(L), Honey template(j)←w(j)*
7. ***end for***
8. *end procedure*

EXPERIMENTAL RESULTS

The facial photos used in this investigation. 500 photos of humans from various racial groups, including South East Asian, Middle Asian, West Asian, and European, are used to train PCA. After training, PCA performs the feature extraction process for all the facial images input. A feature vector B of size 200 is the result of the feature extraction process; The FRR measures the likelihood that the authentication system would wrongly deny authorised users' access requests. FAR refers to the likelihood that an unauthorised user's access request would be inadvertently granted by the authentication system. Each test subject has 20 photos with various facial expressions. We gather 220 people's data. False acceptance rate is used to assess the proposed biometric authentication system's recognition accuracy. and the rate of false rejection (FRR) In this experiment, FAR is calculated by comparing each individual person's image to all 219 other person's images. This procedure is repeated for 220 individuals. Each fruitful match counts as a deceptive acceptance. With regard to FRR, we contrast each photograph of a certain person with the remaining 18 images of him. This procedure is repeated for a total of 220 people. Each unsuccessful match counts as a false rejection. From this, as shown in Figs. 9 and 10, we have FAR and FRR in 2 situations. The FAR and FRR in the absence of biometric template protection are shown in Fig. 9. The initial vectors of biometric features are contrasted with one another. The FAR and FRR are shown in Fig. 10. if our hybrid biometric template protection is being used. The FRR and FAR meet at the threshold in the first scenario shown in Fig. 9. The mistake rate at this crossing is roughly 9%. The equal error rate remains at 9% in the second scenario shown in Fig. 10. These numbers demonstrate that when security is improved, the authentication system's recognition performance is maintained.

$$\boldsymbol{Y} = (\mathbf{8}, \mathbf{2}, \mathbf{1}, \mathbf{13}, \mathbf{21}, \mathbf{5}, \mathbf{9}, \mathbf{6}, \mathbf{22}, \mathbf{7})$$

$$z_1 = med(1,1,8,2,1) = med(1,1,1,2,8) = 1$$
$$z_2 = med(1,8,2,1,13) = med(1,1,2,8,13) = 2$$
$$z_3 = med(8,2,1,13,21) = med(1,2,8,13,21) = 8$$
$$z_4 = med(2,1,13,21,5) = med(1,2,5,13,21) = 5$$
$$z_5 = med(1,13,21,5,9) = med(1,5,9,13,21) = 9$$
$$z_6 = med(13,21,5,9,6) = med(5,6,9,13,21) = 9$$
$$z_7 = med(21,5,9,6,22) = med(5,6,9,21,22) = 9$$
$$z_8 = med(5,9,6,22,7) = med(5,6,7,9,22) = 7$$
$$z_9 = med(9,6,22,7,1) = med(1,6,7,9,22) = 7$$
$$z_{10} = med(6,22,7,1,1) = med(1,1,6,7,22) = 6$$

$$\boldsymbol{Z} = (\mathbf{1}, \mathbf{2}, \mathbf{8}, \mathbf{5}, \mathbf{9}, \mathbf{9}, \mathbf{9}, \mathbf{7}, \mathbf{7}, \mathbf{6})$$

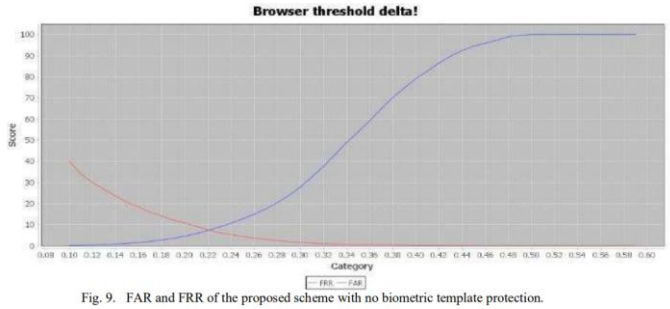


Fig. 9. FAR and FRR of the proposed scheme with no biometric template protection.

Conclusion

While irreversible and unlinkable templates based on Bloom filters are used for protected biometric verification, the honey templates approach is utilised to detect stolen templates. According to the performance assessment, verification accuracy was maintained in comparison to the original unprotected system. A thorough classification analysis was also done to demonstrate how similar the honey and sugar templates are, even if a potential attacker also had access to the secret key used to compute the templates. To this point, additional experimental work must be conducted in the future to enhance the indistinguishable of templates, honey template construction, feature selection methods, or other classification techniques used. Also, the security of

the system was strengthened and the irreversibility of all sweet templates was confirmed: rebuilt templates display HDs to their corresponding original templates that are larger than actual templates that belong to other subjects.

Further enhancements to features like high performance and low computational costs are planned.

REFERENCES

[1] Jain, A.K., Ross, A., Prabhakar, S.: 'An introduction to biometric recognition', IEEE Trans. Circuits Syst. Video Technol., 2004, 14, pp. 4–20

[2] Jain, A.K., Flynn, P., Ross, A.A.: 'Handbook of biometrics' (Springer, 2008)

[3] Jain, A.K., Nandakumar, K., Nagar, A.: 'Biometric template security', EURASIP J. Adv. Signal Process., 2008, 2008, pp. 1–17

[4] Cavoukian, A., Stoianov, A.: 'Biometric encryption in encyclopaedia of biometrics' (Springer Verlag, 2009)

[5] Rathgeb, C., Uhl, A.: 'A survey on biometric cryptosystems and cancelable biometrics', EURASIP J. Inf. Secur., 2011, 2011, (3), doi: 10.1186/1687-417X-2011-3

[6] Uludag, U., Pankanti, S., Prabhakar, S., et al.: 'Biometric cryptosystems: issues and challenges', Proc. IEEE, 2004, 92, (6), pp. 948–960

[7] Ratha, N., Connell, J., Bolle, R.: 'Enhancing security and privacy in biometrics-based authentication systems', IBM Syst. J., 2001, 40, (3), pp. 614–634

[8] Juels, A., Rivest, R.L.: 'Honeywords: Making password-cracking detectable'. Proc. ACM SIGSAC Conf. on Computer and Communications Security, 2013, pp. 145–160