Comparative study of computer simulation software's

Abolfazl mostafaee , S.Hossein Hosseini Nejad
Department of Computer Engineering. Ahar Branch, Islamic Azad University, Ahar, Iran.
E-mail: abolfazlmostafaee1@gmail.com, s.hosseininejad@gmail.com

Abstract

Nowadays, walking is considered as an efficient biometric feature for user authentication. Although there are some studies that address the task of securing gait patterns in gait-based authentication systems, but they do not take into account the low discrimination and high diversity of gait data, which significantly affects the security and practicality of the proposed systems. In this article, we focus on addressing the above shortcomings in the inertial sensor-based gait system. In particular, we use linear discrimination analysis to increase the discrimination of gait patterns, and use the amount of gray code to extract a high, differential, and stable binary pattern. Experimental results on 38 different users showed that our proposed method significantly improves the performance and security of the gait encryption system. Specifically, we obtained a false acceptance rate of 6 × 10−5 (for example, 1 failure in 16983 experiments) and a false rejection rate of 9 2 with 148-bit security.

Keywords: Biometric Security - Authentication - Encryption - Gray Code

1. Introduction

Information security is currently one of the most important issues that has been considered by many researchers. Two techniques are widely used to achieve security. These techniques are nothing but cryptography and cryptography. Encryption can be a way to secure key information. In this method, the sender encrypts the message with the help of a key. The recipient decrypts the message sent by the sender after receiving it to extract the encrypted information from the message. Encryption focuses on keeping the content of the message secret. Cryptography is the act of hiding information from the viewer of the message. This method relies on an encrypted message and hiding it in the transfer layer. So that it is hidden from the observer in the message transmission path. The important point is that there is no secret message transfer layer in the file transfer layer and therefore it can be seen by observers. The power of cryptography is to hide encrypted messages in a non-secret file. When hiding information (cryptography) focuses on keeping the message hidden. Information cryptography is one of the secure communication techniques. Hiding information involves hiding data. So that no data seems to be hidden. If one or more people see the file where the information is hidden, they will not realize that there may be information in it. For this reason, they will make no attempt to decrypt the information. Hiding information is the process of hiding a message covering files such as photos, videos, text and audio. Hidden image has many applications, especially in the technologies of today's modern world. Privacy is a concern for many people on the Internet.

With the rise of the Internet and the means of electronic communications, electronic security and the secrecy of information are becoming increasingly important. In order to protect important information, it must be formatted so that it is not easily accessible to everyone and can only be decrypted by certain people. This process is called encrypting information conversion. Encryption is used to protect emails, credit card information and company data and other important and confidential information. Algorithms called cryptographic algorithms are used to encrypt and decrypt important and confidential information. Because basic management is an important foundation of a secure mechanism, it is always an up-to-date research topic. This is still the most difficult aspect of cryptographic security. At present, researchers have not found the ideal solution to this problem. Light encryption algorithm or higher sensor node performance is still not applied. As a result, the large-scale sensor network always remains operational.

Network security issues have received more attention and become an important point and create problems in the field of network environment research. Information and network security must be met with features such as identification, reliability, integration and Undesirability, and so on.

IOT will be applied to important areas of the national economy, such as health care and medical care and smart transportation. As a result, security in the field of IOT is more important in terms of accessibility and dependency. With the development of WSNs, radio frequency detection (RFID) pervasive computing technology, network telecommunications technology, and instantaneous distributed control theory, CPS has become an emerging form of IOT. In this system, high security is required to ensure the performance of the system. As mentioned, security challenges for IOT have been met. Creating quasi-secure structures is also essential. Basic management in a real large-scale sensor network is always a challenge, and the rules and regulations in this area, which are related to IOT, are also among the challenges. Generally, symmetric encryption algorithms are used to encrypt data for reliability such as the advanced encryption standard; Asymmetric algorithms are also used for digital signature and transfer applications. ECC compliance has also declined and may be welcomed in recent applications.

In order to use these encryption algorithms, available resources such as CPU speed and memory are required.

As a result, it is not clear how these cryptographic methods are applied in IOT , and further research is needed to confirm that algorithms can be well exploited using limited memory and low-speed processors in IOT .

2. Thematic literature of Research

Cryptography is the knowledge that examines and recognizes the principles and methods of transmitting or storing information securely (even if the data transmission path and communication channels or the data storage location are insecure). Cryptography is the use of mathematical methods to establish information security.

Basically, cryptography is the knowledge of changing the text of a message or information with the help of a password key using a password algorithm. In such a way that only a person who knows the key and the algorithm can extract the main information from the encryption information, and a person who does not know one or both of them cannot access the information. The knowledge of cryptography is based on principles such as information theory, number theory and statistics and is studied and used specifically in telecommunications science today.

The word Cryptography is derived from the two Greek words Kryptos meaning "confidential" and Graphien meaning "writing". Symmetric key encryption systems use the same key to encrypt explicit text and decrypt encrypted text. Symmetric key systems have the advantage of being simple and fast.

However, an important factor to consider is that the transfer parties must exchange the key securely.

Data encryption using AES consists of seven cycles depending on the cryptographic blocks, 128-AES, AES-192 and AES-256. A typical cycle in AES encryption involves 4 sub processes. The decryption process of an AES encrypted text is similar to the encryption process but in reverse.

Each round consists of four processes that are performed in the opposite direction:

* Add round key
*Collapse columns
*Move rows
* Replacing bits

Because the sub processes in cryptography and decryption are in reverse order in each round, however, unlike a Faistel cryptography, cryptography and decryption algorithms, although highly interrelated, must be implemented separately. Perceptual nodes are generally smaller in computing power and storage capacity because they are simpler and consume less power.

As a result, they are unable to apply the desired telecommunication frequency and the main public encryption algorithm for secure protection. Therefore, creating a secure protection system is very difficult. At the same time, attacks from external networks, such as lack of access to the network, also create new security issues.

On the other hand, sensor data still needs protection for integration, detection and reliability.

Although the central network is fully secure, human attacks and fraudulent attacks still exist, and unsolicited e-mails and computer viruses cannot be ignored, and large volumes of data can cause congestion.

As a result, the security mechanism at this level is very important in IOT. Support layer: is responsible for heavy data processing and intelligent decision-making of network behavior, intelligent processing for fake information is limited. Because there is a challenge to improve the ability to detect unwanted and fake information.

At this level, security is different for different application environments, and data sharing is one of the characteristics of the application layer, which causes problems with data privacy, access control, and information disclosure.

3. Argument and the Place of Importance of the Research Topic

Walking is considered as an efficient biometric feature for user authentication.

There are some studies that address the task of securing gait patterns in gait-based authentication systems. But they do not take into account the low discrimination and high diversity of gait data, which significantly affects the security and practicality of the proposed systems. In this research, we focus on addressing the above shortcomings in the inertial sensor-based gait system. In particular, we use linear discrimination analysis to increase discrimination in gait patterns. And to extract a high and stable binary pattern, we will do the grading of the gray code.

Experimental results on 38 different users showed that our proposed method significantly improves the performance and security of the gait encryption system.

4. Research Background

With the continued development of the global economy, the market situation becomes more complex and it becomes more difficult to decide on the investment of companies.

As the most important decision in all the decisions of a company, mistakes in investment decisions will lead to great losses for the company. An investment decision usually refers to an investment decision made by an investor after researching, analyzing, and presenting a company or project. Therefore, how to understand the accurate analysis of the investment outlook has become the focus of research by many researchers. Wey studied the optimization framework for investment decisions for renovation with the aim of saving energy in several buildings under limited budget (Wei 2020) Also a multi-objective optimization model with economic goal as net present value and profit time and environmental goal as energy saving goal and emission reduction and design of an intelligent optimization method by combining particle swarm optimization and genetic algorithm, Suggested a search for investment strategies for change. (Minhaj Ahmad Khan-Khalid Saleh, 2018)

GAO developed a theoretical model of analysis based on the rules of intuitive reasoning, which uses financial analysts' stock reports as input and creates portfolio strategies through evidence-based portfolios (GAO 2019).

Sevastianov and Dimova present Dempster-Schaffer theory and fuzzy set theory in an expert business system that simulates the human decision-making process. They also offer suggestions for traders to buy and sell stocks or other financial instruments, taking into account factors such as price history, technical analysis indicators, and well-known trading rules. (Erfan Movahedini, Ahmad Al Morgan, Mohammad Mehdi Hassani, 2019.)

Chou combines a new cost-effective loan forecasting model with a specific investment decision model in the P2P loan market. (Sijari, Rizardi, Grecio, Kevin Poricini, 2015.)

The practical contribution of this model is to provide a complete loan forecasting mechanism based on fuzzy support vector device and use a simple regression model to rank high-yield loans and ultimately high-grade portfolio loans. The advent of IOT technology enables real-time access to project or enterprise data. (Baqalzadeh, Nazial and Sajjad Nemati Pouya, 2016)

In the last decade, the Internet of Things has been the focus of much research. Security and confidentiality are important issues for IOT applications and continue to face major challenges.

The most important issue related to IOT security is the issue of data authentication and comprehensiveness. Because authentication usually requires the proper servers and infrastructure to exchange messages between different components, it is difficult to provide it in the Internet of Things.

To examine IOT security in this article, we first consider a four-tier criterion for IOT and then explain the appropriate security solutions for each layer.

Given the above, this article briefly examines a number of IOT security methods such as encryption mechanism, secure telecommunications, sensor data protection and encryption algorithms.

Among the existing methods, more attention has been paid to the study of Hoffman cryptography and the efficiency of this method for establishing security in IOT.
(Baqalzadeh, Nazial and Sajjad Nemati Pouya, 2016)

Today, the architecture of the Internet needs to be reviewed and updated to connect the trillions of devices and ensure interoperability between them.

However, the most important issue in this area is IOT security requirements, which is probably one of the main reasons for the relatively slow development of this field.

This article presents the most important application layer protocols currently used in the field of IOT: CoAP, MQTT, XMPP. In general, IOT operations consist of three distinct stages:

Collection, transfer, processing, management and processing (Borgia 2014)

Conventional security countermeasures cannot be applied directly to IOT technologies due to different standards and volumes of existing communications. In addition, the large number of connected devices raises the issue of scalability.

Therefore, a flexible infrastructure is needed that must be able to deal with security threats in such an indoor environment. (Sijari, Rizardi, Grecio, Kevin Poricini, 2015)

An article examines the standard advanced encryption method, or AES for short, that can be used both in software and hardware, for use in the Internet of Things. The use of this algorithm in hardware implementation is very important in order to reduce production costs, increase operational capacity and reduce power consumption. (Moslehi, Mohammad and Mostafa Ghobaei Arani, 2016)

The growth of body area networks (BANs) has attracted widespread attention in scientific and industrial research, as the concept of BANs provides a solution for real-time health monitoring. Meanwhile, Vehicle Networks (VANs) support communications in smart vehicles and intelligent traffic systems. In practical situations, the two domains overlap in different situations, and their combination can provide a variety of services that take advantage of their complementary nature. (Junchaio Wang, Keining, Pang, Guangil, 2018)

Cloud computing provides highly scalable and flexible computing and storage resources for payment policies for all three applications. Cloud computing services are becoming more and more common for computing and storage, and many organizations are now moving their data from in-house data centers to cloud storage providers (CSPs). However, increasing user base and remote data storage poses challenges such as inefficient use of resources and insider threats to data rest in cloud storage. (Erfan Movahedini, Ahmad Al Morgan, Mohammad Mehdi Hassani, 2019) In one paper, he proposed an encoding system for speech signals based on circular changes in rows and columns. This cryptographic system uses three secret keys. The master key is generated randomly using a pseudo-noise sequence generator, and the other two keys are generated using the master key. The encryption system also uses DST to intelligibly remove the signal. In addition, the performance of the proposed algorithm is estimated. (Delila Silmani, Fatiha Marzkani, 2018)

The most important issue related to IOT security is the issue of data authentication and comprehensiveness. Because authentication usually requires the proper servers and infrastructure to exchange messages between different components, it is difficult to provide it in the Internet of Things. For this purpose, in an article on IOT security, first a layer criterion for IOT is considered and then the appropriate security solutions for each layer are explained. (Baqalzadeh, Nazial and Sajjad Nemati Pouya, 2016)

Research has addressed the security needs of the Internet of Things along with attacks, threats, and innovative solutions. In addition, IOT security issues are tabulated and mapped with solutions found in other related articles. (Minhaj Ahmad Khan-Khalid Saleh, 2018)

Encryption is an integral part of the information security of the modern world that makes the virtual world a more secure place. Cryptography is a process that makes information incomprehensible to an unauthorized person. In this way, it provides privacy to real users. There are several cryptographic algorithms that can be used. Ideally, a user needs a low-cost, high-performance encryption algorithm. In reality, however, there is no such algorithm as a complete solution. There are several algorithms that must be evaluated between cost and performance and selected based on the type of application. (Sheng, Sun, Yao 2012)

Encryption is one of the most interesting areas of technology that works by obscuring data, making the data unreadable to unwanted people. The Advanced Encryption Standard (AES), also known as Rijndael, the original name of the AES algorithm, is a technical description of electronic data encryption. Encryption is the process of encrypting sensitive or important messages or information in a way that only legal entities can read. Cryptography does not in itself prevent eavesdropping, but makes information obscure and inaccessible to the listener. (Huang, Nguyen 2015)

Encryption, more simply, means generating encrypted text that can only be read by people who have the key to decrypt it. One such encryption method used to protect online data against any malicious threats is the Advanced Encryption Standard (AES) algorithm. (Morse-Ralph-Fland, 2014).

5. Research Methodology

Research methodology, which selects the appropriate method for each research based on the research topic and its design, is one of the most important parts of the research process.

In this research, the library method has been used to achieve and combine GQC algorithm with cryptography and its improvement. The tested data were used from Idea Pardaz and Noavaran companies. In order to analyze and test the data, help has been obtained from MATLAB software**.**

6. Theoretical Framework of Research

The present study is an applied research that will be done in a combination of quantitative and qualitative methods. To do this, after studying books, articles and various algorithms in the subject area of the dissertation, a new approach to investigate the impact of performance and security of the cryptographic system is proposed. To evaluate it, after simulation, the formulation is done in a suitable software environment and will be compared with other similar algorithms in the evaluation criteria such as reminder, accuracy, precision and F harmonic mean. In the proposed method, after preparing the data set, preprocessing and normalization actions will be performed on it so that the algorithm becomes a standard and processable data set. Walking is considered as an efficient way to identify a person through human movement. The development of Micro Electromechanical technology has opened a new approach to the implementation of gait authentication systems in which gait signals are collected by inertial sensors. This method allows the user to authenticate. Thus, compared to passwords or other biometric systems, it offers significant advantages for use that require the user to authenticate to make explicit moves. Several gait-based authentication schemes have been proposed in the literature.

Despite their merits, all of these studies rely on traditional pattern recognition methods, where gait patterns are extracted. Or the models are stored locally without protection of confidentiality, which may cause security and privacy problems for the user if such raw data is compromised by an attacker. To address the biometric data privacy concerns, several studies using the Biometric Cryptosystem have been proposed. One of the most common techniques recently used to protect biometric patterns is the fuzzy commitment scheme. Where a binary string is extracted from biometric patterns and then attached with a key encrypted by the error correction code (ECC) before you write in stock despite the fact that such designs provide a beautiful strategy for Privacy offers biometric patterns, but they did not consider biometric behavioral features such as walking, which are known to be less discriminating and highly unstable. As described in [20], these issues can reduce the security and performance of the FCS-based system. For example, key length, false acceptance rate (FAR), false rejection rate (FRR) where a differentially extracted binary string may lead to high FAR. While an unstable state can lead to high FRR and low security. Therefore, it is critical to develop a method that can extract distinct and stable strands from gait patterns to improve the security and performance of the gait encryption system.

In this research, we propose methods to address the above shortcomings to improve the security and cryptographic performance of the inertial sensor-based gait system. These methods are as follows:

* First, we address the problem of low discrimination and high diversity of gait data by adopting discriminatory linear analysis. Because traditional LDAs are not compatible with FCS, we recommend an LDA modification to do the following:

1. Improving the ability to separate walking data from different users
2. Reduce the diversity of walking data from the same user
3. Preserve the above feature dimensions of gait data for sufficient extraction of the binary string for use in FCS.

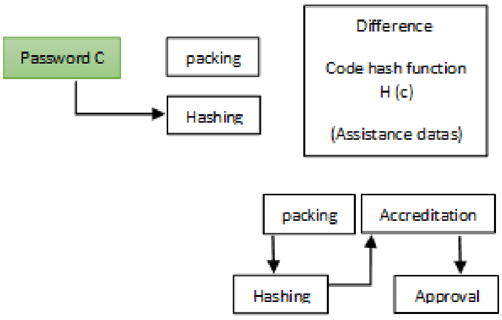
* Second, we propose the gray code which is the same as the quantization scheme.

This design can have a high ability to tolerate error and can be used to reduce gait patterns after the LDA design to the binary pattern.

* Third, we design a method that can determine the reliability of each component in the extracted binary pattern.

Highly reliable components will be selected to form the final binary string input for the FCS.

Finally, we conduct a comprehensive test to analyze the performance of the proposed techniques and perform a detailed security analysis to assess the security of our system against various attacks. We obtained with 5-10 × 6 FRR, (For example, 1 failure in 16983 experiments), 9.2% FRR with 148 bit security. This experimental result showed that the proposed methods not only increase security, but also significantly improve the performance of the gait cryptography system compared to other works of art. The Fuzzy Commitment Scheme (FCS) is a general BCS framework proposed by Jules and Wattenberg that uses the ECC error correction code to control changes in biometric data. The basic idea of FCS is to express each control bit ω (for example, a biometric pattern) in the form of a password C ∈ c with length and a compensation 0 ∈ {δ ‹n} 1 so that δ ⊕ is a ∈ ω where C and FCS error correction in two steps Which is drawn in the following figure:



Registration step: The password C ∈ c is randomly selected and its hash value or (H) is calculated. Step 1.1. Meanwhile, c is sealed to δ by the biometric pulse ω (step 2,1.) The hash values H (c) and δ are stored as auxiliary data for authentication while c and ω are discarded.

Authentication step: According to the ω biometric pattern, the password c is estimated.

It is retrieved using the auxiliary data δ (step 1,2). Then its hash value (c) is calculated (Step 2,2.) Finally, H (c) and c(H) corresponds to make the final decision. (Step 3.2)

As discussed in [18], each c key in C has two parts as length information (k (k / u003cn) and an extra length (k - n). The ratio between the value of two parts in c is between the strength of security and resistance. The system is more secure as the information part expands. Asymmetry makes the system more resilient as the extra part increases.

7. Fisher Distinctive Linear Analysis

Linear Analysis (LDA) is a data reduction method that stores as much discrimination information as possible. Assuming that an X training dataset contains classes D, each has Ni patterns.

The LDA finds a W to convert X to Y as X WT = Y so that variation within the class is minimized and discrimination between classes in Y is maximized. Let x be the mean vector of X and i ¯x be the mean vector of the class patterns Li. Then the scattering matrix of class Sw and between the scattering matrix of class Sb are calculated as follows:

$$(Sw) = \sum_{i=1}^{D}\sum_{j=1}^{ni}(xij - xi)(xij - xi)^{T}$$

$$(Sb) = \sum_{1i=1}^{D} Ni\,(xij - xi)(xij - xi)^{T}$$

Where xij is the pattern j of the class Li. The projection matrix W is the result of the maximization problem using the Fisher criterion.as:

$$\left(Sb\right) = \sum_{1i=1}^{D} Ni \left(xij - xi\right)\left(xij - xi\right)^{T}$$

The optimization task (3) is equivalent to the generalized special problem egen described in [32] and is as follows: When Sw is non-singular, W is the column content whose columns are the specific vectors of maximum (1-D) which are the largest eigenvalues of w1Sb− S.

Software has been used to simulate and implement the proposed method.

MATLAB is a software environment for numerical calculations and a fourth-generation scripting language. The word MATLAB means both a digital computing environment and the corresponding programming language itself, which is a combination of the words MATrix and LABoratory. This name represents the program-based matrix approach in which even single numbers are considered as matrices. Working with matrices in MATLAB is very simple. In fact, all data in MATLAB is stored as a matrix.

8. Research Data Set

We used the data set in [12] for experimental analysis of the proposed system. The dataset contains 38 user walk signals. We extracted the walking signals to 10224 gait patterns using the process in Section 2.3. For experimental analysis, we have developed an authentication model for each user. In each model, we consider one main user and the rest are fake. In the registration step for each user, we form the G matrix containing N = 100

The main user gait patterns and the remaining data is used to validate the model built in the authentication step (12 templates for each effort) (In the LDA training phase, we divided the main data space into 15 sub-spaces S = as described in Section 3.3. We chose the password length of 255 BCH and 511 bits. To understand the effect of such parameters, we analyzed the system with different quantification bit values and k-key lengths.

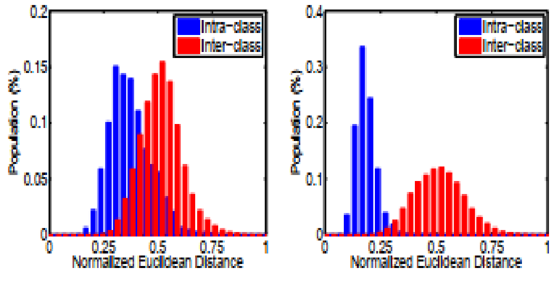
To evaluate the performance of our proposed system, we used the False Acceptance Error Rate (FAR) and the False Non-Acceptance Error Rate (FRR) as standard criteria. Finally, we analyzed the security of our system against various attacks.

By setting the 4-bit Gray code, we have the optimal result. Figure 3 shows the FAR and FRR with different key lengths and BCH codes. Using the 255-bit encryption key and the 87-bit key, the system achieves 0% FAR and 9% 8R FRR. With a 511-bit encryption key and a 148-bit key, 2 2.9 FRR ٪and 10−5 × 6 FAR) (for example, 1 experiment in 16983 experiments). Under various attacks, the system security is 875 and 148 bits with 255 and 511-bit code, respectively.

9. Simulation Parameters

Most algorithms have parameters that need to be adjusted during the simulation phase.

We used the normal Euclidean distance [35] to analyze the effect of the LDA design on gait pattern discrimination. Figure a4 shows the normal Euclidean distance distribution of the gait pattern before the LDA design. We can see that the overlap area within the classroom and between classes is significant. After the application of the modified LDA, the overlap area is significantly reduced, as shown in Figure 4. The normal distribution of Euclidean distance from gait patterns before and after the LDA scheme.



(a) Before LDA projection

(b) After LDA projection

This contrast reflects the effect of the modified LDA presented in Section 3.3.

The LDA prediction phase plays an important role because it increases data discrimination and thus significantly improves system performance.

10. The Effect of Gray Code Quantification

We used the normal Hamming distance to analyze the effect of Gray code quantification.

Because gait signals are unstable, a specific component of the gait pattern can have different values at any time during sampling. However, if these values still belong to the same quantum, the system leads to the same binary string. Using Gray code quantification can minimize error bits when these values are placed in different quanta. Therefore, using Gray code provides a higher fault tolerance capability to increase performance, and the number of a-bit values is switched between the FAR and FRR values of the system. The quantum amplitude φ decreases with increasing aces and vice versa. Given that Ψ is small, (So φ is large), probably the same binary string can be extracted from two different gait patterns. As a result, the Hemming distance between the class and the inside of the class is reduced, as shown in Figure 5.

This leads to an increase in FAR and a decrease in FRR. Figure 6 shows a comparison of the Hemming distance distribution between the use of 4-bit binary code and the quantification of 4-bit bit code. When using the Gray code (Figure 6 c, d,) the Hamming distance within the class is much shorter than using the natural binary code (Figure 6 a, b.) Table 1 is the Comparison of 3-bit and 4-bit gray code quantification in terms of FRR, FAR in the same word length code and key length. We can see that when 3 = FRR, FAR is higher than 4 = Ψ.

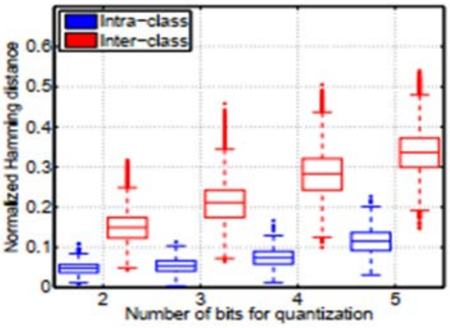
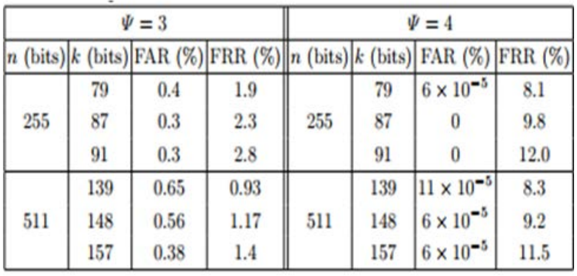


Fig.1. Hamming distance distribution when using different values Ψ to determine the Gray code value



$\Psi = 3$				$\Psi = 4$			
n (bits)	k (bits)	FAR (%)	FRR (%)	n (bits)	k (bits)	FAR (%)	FRR (%)
255	79	0.4	1.9	255	79	6×10^{-5}	8.1
	87	0.3	2.3		87	0	9.8
	91	0.3	2.8		91	0	12.0
511	139	0.65	0.93	511	139	11×10^{-5}	8.3
	148	0.56	1.17		148	6×10^{-5}	9.2
	157	0.38	1.4		157	6×10^{-5}	11.5

Table 1.The system performance is related to the word length code n, key length k and number of quantization bits

11. Research Evaluation Criteria

In this section, we analyze system security against several statistical attacks. A typical attack, brute force or sweeping search attack is a random key. One of the penetration testing methods that threatens many services on a daily basis attacks are used by many hackers, it is an attack in which all possible cases are investigated until the answer is reached. [1]

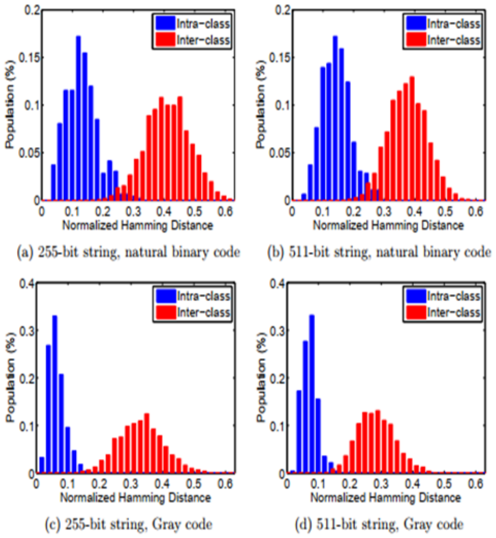
If you go to a site like Instagram, you will see a login page for you and it means that through this page and the existing form to your account. Sign in, but if we want to look at this page from the perspective of a hacker or cracker, we can hack into different user accounts.

For each cryptographic pattern, the time required to test all possible states for the key can be calculated, and cryptographic patterns are usually designed in such a way that it is impossible or ineffective to test all possible states at an acceptable time.

Also, "pervasive search attack" is a criterion for recognizing methods of decryption, which means that any method that can unlock the password faster than "pervasive search" method is considered a method of decryption. Testing all possible modes is also used as a way to find the password. Typically, software blocks a user's account after entering incorrect passwords several times, or delays the validation process to prevent other modes from being tested. In some cases, the words of a dictionary are tested as a possible way to crack the password, which is called a "dictionary attack". This is because users are more likely to choose meaningful words for the password than to choose meaningless words. A comprehensive search attack works by calculating and testing all possible modes, each of which can form a password. As the password length increases, the time to find the password increases exponentially on average. Since the suggested key lengths are 87 and 148 bits for the 255-bit and 511-bit code words, the security strength against the key attack is 87 and 148 bits, respectively.

We analyze whether an attacker can misuse auxiliary information including Wi-Fi prediction matrices, minimums, maximum vectors for normalization, acceptable component indices p, δ, and hash code H (m). Maximum vectors contain maximum statistical information from the entire data set and, therefore, are not user-specific.

Therefore, the maximum vectors do not represent the maximum information about the original user. The reliable component index vector p contains only information about the discrimination and stability of gait patterns. Such indicators do not show information about the biometric pattern. Therefore, it cannot be used to return to the biometric pattern. Using the hash code (m) H, due to the performance of the cryptographic graphical hash, the attacker cannot return to m with an unavoidable probability.



(a) 255-bit string, natural binary code (b) 511-bit string, natural binary code

(c) 255-bit string, Gray code (d) 511-bit string, Gray code

Fig. 2. Hamming distance distribution of reliable 255, 511-bit strings when using natural binary code and gray code with 4-bit quantification.

LDA projection matrices are not user-specific because they only reflect information about the population of the data set. In addition, the projection matrix is formed by special vectors Sw λ Sw-1Sb. From λ, we cannot return to Sw-1Sb without knowing the corresponding specific values, which are discarded immediately after the LDA training phase. Therefore, from the stored special vectors, we cannot return s-1w Sb and obtain the original biometric patterns of the registered user. Using secure δ, to obtain the m key, the attacker can guess a string hidden in δ that is close enough. The distance depends entirely on the BCH code error correction capability and uncertainty, which depends on the quantization method.

We use entropy to measure uncertainty. We calculate the entropy of each bit with the following formula**.**

$$\boldsymbol{(wi) = -\mathrm{pi}\log(pi) + (1 - pi)\log(1 - pi)}$$

Where 1 = ((i!) Pr = pi) is the probability of obtaining the i-bit value i due to quantization. Entropy E reliable string! By summing the entropy, all components are calculated as

(i!) H 1 = i Pn = E). Due to the quantification of the Gray code, the probability of receiving a value of 1 bit 5 0 = pi i. The system then obtains the entropy of 250 E and 500 for codes 255 and 511, respectively. The security of the system against this attack is measured by the Sphere package according to [10]

$$\boldsymbol{Csb} \geq \mathbf{2\ E} \,/\, \sum(\boldsymbol{E})$$

That t is the error correction capability. For the two suggested key lengths of 255 bits and 511 bit code words, error correction capability, respectively 26 and 53 bits are like [22,]

So it gets the CSB system as 2133 and 2269.

Conclusion

The resources required for a pervasive search attack increase exponentially (not linearly) as the key length increases. Although US export regulations have restricted key lengths to 56-bit symmetric keys (eg data encryption standard). But these limitations are no longer in place, and the usual modern symmetric algorithms are the keys that we can use 128 to 256 bits more powerful. According to a physical argument, **128**-bit symmetric keys are computationally safe against a pervasive search attack.

Based on the laws of physics, the Landau limit principle states that to clear each bit of low-limit information, the energy required is obtained from the formula Ln**2** * kT, where T is the temperature of the calculator in Kelvin and k is the Boltzmann constant. Also, the natural logarithm of number **2** (logarithm **2** based on e) is equal to **0.693**, and no irreversible computing device can consume less than this energy. So in order to be able to guess the possible values for **128** symmetric bits (without doing the actual calculations to find it) you theoretically need **1 - 2128** bits on a typical processor.

Assuming that the calculations are performed at a temperature close to room temperature (**300** K), the energy required to do so can be calculated using the Neumann-Al-Nadawa law.

This energy is approximately equal to 1018 joules, which is equivalent to consuming 30 gigawatts of power per year. This amount of energy is equal to:

W × 365 × 24 × 3600 s = 9.46 × 1017 J or 262.7 TWh 109 × 30

More than one percent of the world's energy (Complete calculations - to check each key - consumes this amount of energy many times. This value is only the amount of energy required to travel the key state space and the time required to change the herbit is not considered, which is certainly more than 0. However, this argument assumes that the values of the registers are changed using conventional insertion and clearing methods that inevitably create entropy. Research has shown that computing hardware can be designed to meet this theoretical limitation - see Reversible Computing -

However, such computers have not yet been built. We analyzed the statistically attacked system based on the extracted reliable string Hamming distance distribution. In particular, the enemy can extract a reliable string from its gait signal. Then, with the distance between Hamming class as h, he knows he can guess the string. In addition, using the error correction feature of the BCH code as t, he just has to search everyone! So that h-t=(!dH)!0 is safe to retrieve the key m from safe d. Let h- t = d, so the cost of this attack is equal to:

$(h) = (n, d) = n!/\, d!\, (n - d)!$

We assume that h follows the Gaussian distribution. We estimate the mean hand variance σh of the clock in Figure 6. Then, we analyze h (CST) with h in (2σh - μh) and (2σh μh) using (13). With 4-bit quantification, the security power is 108 and 235 bits, respectively, which corresponds to 255 word and 511 bits, respectively. If an attacker attacks offline and has access to encrypted expressions, he or she can test key combinations to find the correct answer without risking external interference or exposure.

However, database administrators can retaliate against online attacks. For example, by limiting the number of times a password can be entered or creating a time delay when entering it repeatedly, or complicating the response - for example, using Capcha or send the verification code to the mobile phone and ...- or lock the account after several failed attempts (entering the wrong password).

Webmasters may also block and restrict an IP address that logs in more than the specified number of times and enters a password on that site.

Acknowledgments

If necessary.

References

[1] Baqalzadeh, Nazila and Sajjad Nemati Pouya, (2016), IOT Security, Second National Conference on New Approaches in Electrical and Computer Engineering, Khorramabad, Islamic Azad University, Khorramabad Branch.

[2] Moslehi, Mohammad and Mostafa Ghobaei Arani, (2016), An Approach Based on AES Encryption Algorithm for IOT Security, 3rd National Conference on Electrical and Computer Engineering of Distributed Systems and Intelligent Networks, Kashan, Islamic Azad University, Kashan Branch.

[3] Security, privacy and trust in Internet of Things: The road aheadS. Sicari a, , A. Rizzardi a, L.A. Grieco b, A. Coen-Porisini ,"Computer networks*",ELSEVIER*,76(2015) pp 146-164

[4] Junchao Wang,Kaining Han,Anastasios Alexandridis,Zeljko Zilic,Yu Pang,Wei Wu,Sadia Din,Gwanggil Jeon, *"Computer Networks*" - Volume 143, 9 October 2018, Pages 74-81

[5] Irfan Mohiuddin,Ahmad Almogren,Mohammed Al Qurishi,Mohammad Mehedi Hassan,Iehab Al Rassan,Giancarlo Fortino, "Future Generation Computer Systems "- Volume 90, January 2019, Pages 307-316

[6] Dalila Slimani,Fatiha Merazka, Procedia "Encryption of speech signal with multiple" secret keys - Volume 128, 2018, Pages 79-88

[7] Wang Wei,Si Miaomiao,Pang Yu,Ran Peng,Wang Huiqian,Jiang Xiaoming,Liu Yu,Wu Jun,Wu Wei,Naveen Chilamkurti,Gwanggil Jeon, "An encryption algorithm based on combined chaos in body area networks" *Computers & Electrical Engineering* - Volume 65, January 2018, Pages 282-291

[8] C. Rathgeb and A. Uhl. Adaptive fuzzy commitment scheme based on iris-codeerror analysis. In 2010 2nd European Workshop on Visual Information Processing(EUVIP), pages 41,44. *IEEE*, 2010.

[9] Y. Zhao and S. Zhou. Wearable device-based gait recognition using angle embeddedgait dynamic images and a convolutional neural network. Sensors, 17(3):478, 2017.

[10] B. Firner, R. S. Moore, R. Howard, R. P. Martin, and Y. Zhang, "Poster: Smartbuildings, sensor networks, and the Internet of things," in *Proc. ACM Conf. EmbeddedNetworked Sensor Systems*, Nov. 2011, pp. 337–338.

[11] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Securityvulnerabilities and challenges," in Proc. *IEEE* Symp. Computers and Communication,Larnaca, Cyprus, Feb. 2015, pp. 180–187.

[12] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security andprivacy in distributed Internet of things," *Comput. Netw*., vol. 57, no. 10, pp. 2266–2279, July 2013.

[13] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy forcloud-based IoT: Challenges," IEEE Commun. Mag., vol. 55, no. 1, pp. 26–33,Jan. 2017.

[14] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection withreinforcement learning in wireless networks," *IEEE Trans*. Veh. Technol., vol. 65, no.12, pp. 10037–10047, Dec. 2016.

[15] M. Abu Alsheikh, S. Lin, D. Niyato, and H. P. Tan, "Machine learning in wirelesssensor networks: Algorithms, strategies, and applications," *IEEE* Commun. SurveysTutorials, vol. 16, no. 4, pp. 1996–2018, Apr. 2014.

[16] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor,"Machine learning methods for attack detection in the smart grid," *IEEETrans*. Neural Networks and Learning Syst., vol. 27, no. 8, pp. 1773–1786,Mar. 2015.

[17] R. V. Kulkarni and G. K. Venayagamoorthy, "Neural network based secure mediaaccess control protocol for wireless sensor networks," in *Proc. Int. Joint Conf. NeuralNetwork*s, Atlanta, GA, June 2009, pp. 3437–3444.

[18] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM conference on Computer and communications security*, pages 28,36.ACM, 1999.

[19] . H. Kaur and P. Khanna. Biometric template protection using cancelable biometrics and visual cryptography techniques. *Multimedia Tools and Applications*,75(23):16333{16361, 2016.

[20] E. J. Kelkboom, J. Breebaart, I. Buhan, and R. N. Veldhuis. Maximum key size and

classification performance of fuzzy commitment for gaussian modeled biometric sources. *IEEE Transactions on information forensics and security*, 7(4):1225,1241,2012.

[21] M.-H. Lim, A. B. J. Teoh, and K.-A. Toh. An efficient dynamic reliabilitydependent bit allocation for biometric discretization. *Pattern Recognition Journal*,45(5):1960{1971, 2012.

[22] R. H. Morelos-Zaragoza. *The art of error correcting coding*. John Wiley & Sons,2006.

[23] M. Morse, J. Hartloff, T. Effland, J. Schuler, J. Cordaro, S. Tulyakov, A. Rudra, and V. Govindaraju. Secure fingerprint matching with generic local structures. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 84{89, 2014.

[24] I. Natgunanathan, A. Mehmood, Y. Xiang, G. Beliakov, and J. Yearwood. Protection of privacy in biometric data. *IEEE access*, 4:880{892, 2016.

[25] C. Nickel and C. Busch. Classifying accelerometer data via hidden markov models to authenticate people by the way they walk. *IEEE Aerospace and Electronic Systems Magazine*, 28(10):29,35, 2013.

[26] C. Ntantogian, S. Malliaros, and C. Xenakis. Gaithashing: a two-factor authentication scheme based on gait features. *Computers & Security Journal*, 52:17{32,2015.

[27] C. Rathgeb and A. Uhl. Adaptive fuzzy commitment scheme based on iris-code error analysis. In *2010 2nd European Workshop on Visual Information Processing (EUVIP)*, pages 41{44. IEEE, 2010.

[28] C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011(1):3, 2011.

[29] C. E. Shannon, W. Weaver, and A. W. Burks. The mathematical theory of communication. 1951.

[30] W. Sheng, S. Chen, G. Xiao, J. Mao, and Y. Zheng. A biometric key generation method based on semisupervised data clustering. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 45(9):1205{1217, 2015.

[31] H. Sun and T. Yuao. Curve aligning approach for gait authentication based on a wearable accelerometer. *Physiological measurement*, 33(6):1111, 2012.

[32] S. Theodoridis and K. Koutroumbas. Pattern recognition{fourth edition, 2009.

[33] N. T. Trung, Y. Makihara, H. Nagahara, R. Sagawa, Y. Mukaigawa, and Y. Yagi. Phase registration in a gallery improving gait authentication. In *2011 International Joint Conference on Biometrics (IJCB)*, pages 1{7. IEEE, 2011.