République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Ecole Nationale Polytechnique
Département d'Electronique
Laboratoire des Dispositifs de Communication
et de Conversion Photovoltaïque

Thèse de Doctorat

Présentée par **MERMOUL Atef**
Magistère en Télécommunications, Université de Technologie de Baghdad, Iraq

Thème

Chiffrement Basé sur les Méthodes Sous-Espace: Concepts et Etude de Robustesse

''Subspace Based Encryption: Concepts and Robustness Study''

Soutenue publiquement le 05 octobre 2013 devant le jury composé de :

Président :	HADDADI Mourad	Professeur	ENP
Rapporteur :	BELOUCHRANI Adel	Professeur	ENP
Examinateurs :	ABED-MERAIM Karim	Professeur	Polytechnic Orléans, France
	BELBACHIR Hacène	Professeur	USTHB
	REMRAM Youcef	Maître de Conférences/A	USTHB
	BOUSBIA-SALAH Hichem	Maître de Conférences/A	ENP

2013

Acknowledgement

The completion of the work is an opportunity to remember all who have helped me along this long but agreeable road.

I would like to express my heartfelt gratitude to Professor Adel Belouchrani, who is not only supervisor but dear friend. Professor Adel Belouchrani is the one professor/supervisor who made a difference in my life. It was under his guidance that I developed a focus and became more interested in sharing scientific knowledge and helping others in their research. I hope that I can in turn pass on the research values that he has given to me.

He provided me with direction and technical support. His persistence, understanding and kindness helped allowed me to complete the doctorate and encouraged me to go on for scientific research. I doubt that I will ever be able to convey my high regard fully, but I owe him my eternal thankfulness.

Besides my supervisor, I would like to thank my thesis committee: Prof. M. Haddadi, Prof. K. Abed-Meraim, Prof. H. Belbachir, Dr. H. Bousbia-Salah and Dr. Y. Remram, for their encouragement, insightful comments and constructive feedback.

I am grateful for the anonymous reviewers at Journal of DSP (Elsevier) and at the various ISSPA, WOSSPA and DAT conferences for helping to shape and guide the direction of the work with their careful and instructive comments.

To the staff of the LDCCP Laboratory at ENP - Algiers, I am thankful for welcoming me as a friend and helping.

To the head of the Documentation Centre at ENP for her help and kindness.

I would like to thank my family for supporting and encouraging me.

And last, but not least, I must acknowledge my friends Abderrezzak Mourad, Djamel, Hocine, Slimane, Mohieddine, Mahmoud, Mourad, Yacine, Redha, Zwawi, Mohammed and Mohammed Tahar for their encouragement.

إهداء

إلى **والدتي الكريمة**، التي ألغت ما يحق لها في سبيل أن ننشأ نشأة سوية و نكبر على حب الحق و الخير و إجلال العلم و أهله،

إلى **والدي الكريم**، المعلم الصامت الذي ربانا بالقدوة قبل الكلمة و قد يتغاضى عن كل الأخطاء إلا الكذب،

رب ارحمهما كما ربياني صغيرا

إلى **زوجتي الكريمة**، التي ضحت على مدار سنوات لأجل أن توفر لي ظروف استكمال هذا العمل وكانت نعم المؤازر و المشجع، حفظها الله ورعاها،

إلى **زينب لجين و إبراهيم**، هبة الله سبحانه و تعالى في الحياة الدنيا، حفظهما الله ورعاهما،

إلى **أخواتي و إخوتي**، حفظهم الله و رعاهم،

إلى **كل من ساهم** في تربيتي و تعليمي, منذ معلم القرآن الكريم في الكتاتيب,

إلى **من جاهدوا** في سبيل الله فحرروا البلاد و العباد و كانوا سببا في ألا نظل عبيدا و مقهورين و أميين،

إلى **من يقومون بواجبهم** في كل موقع،

إلى من لم أذكرهم لأن ذاكرتي خانتني عند كتابة هذا الإهداء،

أهدي هذا العمل و أشكرهم و جزاهم الها كل خير.

عاطف مرمول

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The rapid growth of digital communications and electronic data exchange makes information security a crucial issue in industry, business, and administration. Modern cryptography provides essential techniques for securing information and protecting data [1]. Among cryptographic techniques, Blind Source Separation (BSS)-based methods have received recently some attention in speech and image encryption fields.

However, from our point of view, BSS-based techniques are more suitable for cryptanalysis purposes rather than for cryptographic ones. This is due essentially to the fact that BSS-based techniques are, by their definition, tools developped to recover a set of independent source signals from their observed mixtures without knowledge of the mixing coefficients [2, 3]. This is, by analogy, the same formulation of the cryptanalysis problem i.e. recovering a plain-text (or a set of plain-texts) from cipher-texts (mixtures of plain-texts and cryptographic keys) without knowing the cryptographic keys (mixing coefficients).

This observation about limitations on using safely, from a cryptographic point of view, BSS-based techniques in cryptographic field gave us a stimulus to develop a new technique which would bypass these limitations. This gives arise to a subspace-based encryption technique which is the core added-value of this thesis. The developped subspace-based technique is applied for speech, image and data signals. Several tests and evaluations are conducted to assess the cryptographic robustness of this technique. An assessment methodology is applied for subspace-based encryption technique to appreciate its quality

and security levels.

1.1 Motivation

There is a growing interest, in recent years, in the use of blind source separation techniques in cryptographic domain. Some research groups through the world are trying to propose new encryption algorithms based on blind source separation (BSS) techniques [4]-[10]. As an example, the intractability of the underdetermined blind source separation problem has been used to present a BSS-based speech encryption.

However, some weaknesses from a cryptographic point of view have been recently published [11]. The already proposed techniques should be discussed in detail together with their drawback induced from the use of the blind source separation like approach. Solutions based on background knowledge acquired from the blind identification field should be proposed to improve the existing BSS-based encryption algorithms. This gives arise to subspace-based encryption methods.

This thesis aims to construct an encryption scheme based on subspace concept and by taking advantge from the feedback acquired from the use of blind source separation techniques in the encryption field.

1.2 Goal

In this thesis, we have focused on studying and analysing the use of the subspace concept by investigating first the opportunity of using blind source separation techniques in the encryption domain. We will be discussing the various constraints related to the performance of these techniques. The main tasks of the project are to survey the current status, identify the limitations of these techniques and propose alternative approaches. The analysis would approach the various aspects of the security of blind source techniques used in the encryption domain and their performance. We are looking forward to provide a new research direction towards subspace-based techniques to bypass the limitations and drawbacks inherent to the BSS techniques used in encryption field. Specifically we would be focusing on the security aspects

of such techniques.

1.3 Methodology

We shall conduct a comprehensive analysis of the use of blind source separation techniques in cryptographic domain. Our approach is goal-oriented in the sense that we study the characteristics of BSS techniques that could be relevant to cryptography requirements. For this purpose, an introduction to both cryptography requirements and BSS techniques is first presented.

Then the use of BSS techniques in cryptographic field is detailed before analyzing whether these BSS techniques fulfill or not the cryptography requirements. This analysis will be conducted using cryptanalysis techniques. In the case where this analysis shows that BSS techniques, in the actual state of the art, partially fulfill cryptographic requirements, efforts will be made to propose a new approach which could bring enhancement at this level, actually, subspace-based techniques.

The subspace-based techniques are first applied in encryption field then feedback acquired from their applications on speech, image and data signals, would be used to conduct a quality and security evaluation of these techniques from a cryptographic point of view. Proceeding this way will give us complementary elements necessary for making a conclusion on the opportunity of using subspace-based techniques in the encryption domain.

1.4 Outline

In this thesis, the work starts with studying the opportunity of using blind source separation techniques in the encrytpion domain. Then, after studying the state of the art of these techniques and their weaknesses, from a crytpographic point of view, obtained from former published cryptanalysis works, a new system based on subspace concepts is proposed. To achieve this goal, the thesis is organized as follows: Chapter 2 introduces a brief background on cryptographical and cryptanalysis techniques beside a general reminder on the key concepts of linear algebra used throughout the work and a description of blind source separation techniques. This description is oriented towards

caracteristiques of blind source separation techniques which are relevant to cryptography domain. A state of the art of the use of blind source separation techniques in encryption field is presented. Particularly, cryptanalysis results of these techniques are given within this chapter.

Starting from the cryptographic weaknesses of blind source separation approach, chapter 3 introduces subspace-based encryption techniques. Our proposed encryption system based on orthogonal subspace concept is studied in detail. An iterative version of the orthogonal subspace scheme is presented. Then, in chapter 4, an oblique subspace-based encryption scheme is presented beside its iterative version. In chapter 5, several tests using cryptanalysis attacks are conducted on both orthogonal and oblique subspace-based encryption systems to evaluate their robustness from a security point of view. Results are discussed in detail in chapter 6 in terms of quality and security. This is achieved by using subjective and objective measurements for quality assessment and security evaluation of the proposed system.

Chapter 7 concludes finally the thesis by giving a summary of the main contributions of the work, the limitations and constraints then gives suggestions for future work and issues.

Chapter 2

Background

2.1 Cryptography

Hiding some information or making it incomprehensive to others is a very old human need. Several means were used to meet this need but the process of putting the bases of a whole science, called nowadays cryptology, started only at the seventh century. If cryptology experienced all this development several centuries before, it is because it met partly quite precise needs of the society/state of that time and even anticipated the future needs in precise fields. Kings needed powerful tools to ensure the confidentiality of their correspondances through the various areas of their kingdoms [12, 13].

Cryptography has been a restricted area controlled only by military and diplomatic entities throughout the world. That is why it had and still has, somewhat, a specific reputation. However, during last decades, the fast development of information and communications technologies causes a widespread use of cryptological tools. It has been implemented in various equipments and devices, by software and hardware means.

On the other hand, even confidentiality has been the main objective of cryptography, other objectives are targeted by this science:

- Data integrity: A message sent over a transmission medium should be check-able, by the receiver, whether it has been altered or modified, fully or partially. Data integrity ensures that the transmitted message has been received actually as it was sent by the sender.

- Authentication: Data origin authentication ensures that there is no sender identity usurpation i.e. the origin of the data is correct. This gives the ability to the receiver to verify data origin. On the other hand, entity authentication provides the guarantee that the sender and the receiver could identify each other during all the process of communications.

- Non-repudiation: Non repudiation ensures that it is impossible to later deny sending and/or receiving a message [1].

Of course, other techniques are used to complement and to enhance the cryptography objectives cited above like public key infrastructure and electronic certification. However these areas are out of the scope of this thesis.

Usually, in the cryptography litterature, the term plain-text is used to refer to the message to be transmitted over communications medium, whatever its nature is. It could be a text, audio, video or data. After encryption, it becomes a cipher-text. A general descriptive equation of an encryption operation is given as:

$$x = E(k_e, p) \tag{2.1}$$

where x is the cipher-text, p is the plain-text, k_e is the key (encryption parameter) and E is the encryption algorithm.

On the receiving side, to recover the plain-text, the cipher-text c is decrypted using a decryption algorithm D:

$$p = D(k_d, x) \tag{2.2}$$

where k_d is the decryption key. k_e and k_d could be either different or the same. It depends on the type of the cryptography system.

2.1.1 Classical cryptography

The objective of classical cryptography is to guarantee the confidentiality of the plain-text to be encrypted and sent to a receiver. The principles of perfect secrecy as shown by C. Shannon, in 1949, in his mathematical treatment entitled "Communication Theory of Secrecy Systems", require that the encryption key length must be at least the same as the plain-text length [14]. The encryption key has also to be randomly generated and used once. This

ensures a perfect secrecy or what it is called "one-time pad" or Vernam cipher.

In classical cryptography, the encryption scheme has always been a symmetric one in the sense that both sender and receiver have to share the same encryption keys before starting exchanging encrypted messages. This requirement procures a high degree of confidentiality in case where the encryption keys have been "correctly" generated and distributed to both sender and receiver.

However, from an operational point of view, the management of such a scheme becomes very hard in the presence of an important number of users, senders and receivers, who have to exchange encrypted messages. This is due to the huge amount of encryption keys that must be generated and distributed to all users. This amount of encryption keys to be shared is $n(n-1)/2$ where n is the number of users. As an example, if there is only a thousand (1000) of users, the number of encryption keys to be generated and shared is 499.500 keys, which is indeed a huge amount of keys.

The generation of such a number of keys does not constitute in itself a constraint because of the availability of several efficient processes, software and/or hardware, of generation of cryptographic keys. The difficulty arises from the complexity of the process to be adopted to ensure "correctly" a secure distribution of such an amount of encryption keys to all users, particularly if these users are located in areas far from each other.

These operational constraints have given arise to another class of cryptography so as to bypass the limitations of classical cryptography.

2.1.2 Modern cryptography

On the other hand, complexity theory constitutes the foundation of modern cryptography. It is based on what is called "computational complexity". The assumptions of modern cryptography are the existence of one-way functions and of true randomness. One-way functions are functions whose inversion is computationally intractable. An important result of modern cryptography is that true randomness can be arbitrarily well approximated by pseudo randomness, i.e., the randomness furnished by classical (as opposed to quantum) computers. Security of cryptographic schemes is demonstrated by reduction

to computational problems whose hardness is an empirical fact.

A property of modern encryption schemes is that they are possibly asymmetric, i.e., different keys are used for en- and decryption. The first published treatment of asymmetric schemes appeared in 1976 under the title "New Directions in Cryptography" by W. Diffie and M. Hellman [15]. The first published implementation of an asymmetric scheme appeared in 1978 and is due to R. Rivest, A. Shamir, and L. Adleman [16].

Cryptographic operators

The traditional occupation of cryptographers is the construction of operators for cryptographic tasks such as en- and decryption, electronic signature generation and verification, and destructive compression of data (data hashing). The traditional occupation of cryptanalysts is the "destruction" of those operators, i.e., the breaking of their intended functionality.

Cryptographic protocols

A more modern occupation of cryptographers is the construction of protocols for cryptographic concerns (e.g., trust, confidentiality, identity, and commitment) by employing cryptographic operators. Such concerns arise in the context of communications in hostile environment. The occupation of hostile communicators (so-called adversaries) is the "destruction" of those protocols, i.e., the breaking of their intended functionality. Adversaries can be passive or active.

Cryptographic algorithms

In a cryptographic algorithm, key generation is the process of generating keys. The same key/different key can be used for encrypting and decrypting. The cryptographic algorithms can be classified into the following principal types of cryptographic algorithms: symmetric cryptography, asymmetric cryptography and cryptographic hash functions.

- Symmetric-key cryptography: is an algorithm, where the same shared key is used for encryption and decryption. Thus, data is kept secret by keeping this key secret. These symmetric-key algorithms can further be divided into block ciphers and stream ciphers. Block ciphers take a

number of bits at a time and encrypt them into a single block. A few examples of block cipher are Skipjack, RC5, DES [17] and AES [18]. Whereas, stream ciphers encrypts each message one at a time. A few examples of commonly used symmetric-key algorithms are Blowfish, RC4, TDES, Twofish, Serpent, DES and AES [19].

- Asymmetric-key cryptography: is an algorithm, where the user uses a pair of keys a public and a private key. This public key is widely distributed among the communicating partners, while keeping the private key secret. Thus, the encrypted message sent to one of the communicating partners can be decrypted by the corresponding private key only. The examples include, Diffie-Hellman, Digital Signature Standard (DSS), Elliptic curve cryptography (ECC), Secure Socket Layer (SSL) and RSA encryption algorithm. Asymmetric cryptography can be further classified into two main branches: Public-key and Digital signatures.

- Public-key is a type of encryption, where a message is encrypted with the recipients public-key and can be decrypted only by the recipient having the respective private key thus ensuring confidentiality.

- Digital signatures is a message signed by sender private key and at the recipient end it can be verified by sender public key, thus ensuring authenticity [19].

  A cryptographic hash function is a transformation that takes input a long string of any length and output is a fixed-size string called hash value. This hash value is a concise form of the long message. These hash functions are used in cryptography for a variety of computational purposed. These hash functions are used in message integrity checks and digital signatures. The two most commonly used hash functions are MD5 and SHA-1 [20].

- A Message Authentication Code (MAC) can be summarized as the cryptographic secure sum of a message. It takes as input a secret-key and an arbitrary-length message, authenticates it and gives as output an authenticated message. The MAC is included in the packet sent. The recipient node must be in the possession of the secret key. It

calculates the MAC and compares it with the received message. This is done in order to verify the messages integrity and authenticity. MACs can be constructed from the cryptographic primitives as hash functions or from block cipher algorithms (OMAC, CBC-MAC) [21].

- Comparison: Symmetric-key algorithms are comparatively less computative than asymmetric-key algorithms. Besides this, symmetric-key algorithms are typically hundreds to thousands time faster than the asymmetric-key algorithm. The disadvantage of a symmetric-key algorithm is the need of a shared secret key with both the communicating partners. These keys need to be distributed safely and need to be changed regularly. Thus, safe key-management which includes selecting, distribution and safety is a known issue.

2.2 Cryptanalysis

Cryptanalysis is the second half of cryptology; science which includes cryptography. The desire of knowing the secrets of other persons or groups which use cryptographic tools to secure their communications gives arise to cryptanalysis. During a long time, the confrontation between cryptography and cryptanalysis was occurring on a pure mathematical ground. Mathematical solutions for securing correspondences were defeated by other mathematical tools [22].

In the earlier cryptographic techniques such as alphabetical substitutions or permutations, cryptanalysis was based on frequency analysis of the used languages.

Except brute force attack which remains the last approach to use because of its time and computing resources consumption, some recent techniques have proven to be very efficient against several cryptographic algorithms. As the cryptographic algorithms become more complex, the cryptanalysis becomes more difficult. To reduce this difficulty, new approaches have taken place [22].

Successful attacks may, for example, recover the plain-text (or parts of the plain-text) from the cipher-text, substitute parts of the original message, or forge the digital signatures [1]. Nowadays, providing evidence that the ro-

bustness of a cryptographic algorithm is not as it was claimed is a successfull attack eventhough it does not recover, fully or partially, any of the plain-text or the encryption key.

2.2.1 A brief historical view

It would be interesting to have a brief view on the history of cryptanalysis. During the campaign of translation of books and manuscripts written in several difficult and old languages, and sometimes in dead languages, there was a pressing need to master all known cryptographic tools and techniques. Some of these books and manuscripts, especially in certain areas like chemistry and magic, contained encrypted paragraphs. This need gave rise to a new science: cryptanalysis [12].

A research group (using modern terminology) under the supervision of Yakoob Ibn Ishak Al-Kindi, known as Alkindus, worked at Bait Al-Hikmah in Baghdad, on decrypting the encrypted paragraphs in order to complete the translation process of all the submitted manuscripts [12].

They were the first to discover and write down the methods of cryptanalysis [23]. Among the 290 manuscripts he wrote in various fields, appears the oldest one which discovered and wrote down the methods of cryptanalysis: Rissalatoon fi istikhradji al mooamma (a writing in extracting the encrypted) [12].

Al-Kindi founded the principles of cryptanalysis. He proposed four methods of decryption: quantitative techniques, qualitative techniques, probable word and letters combination. In his manuscript Kitaboo al-moo amma (book of the encrypted), an important handbook of cryptology even centuries later, Al-Kindi proposed a classification diagram of encryption methods and their related cryptanalysis techniques [12].

On another hand, other conditions supported the emancipation of this new science. Disciplines that were developed at that time, like grammar and mathematics, had considerable contribution. Cryptanalysis had an enormous requirement for tools of analyzing languages in which the encrypted texts were written. This helped the mastering of the qualitative approach in cryptanalysis. As for the quantitative approach, like calculating letters

frequencies of several languages, mathematics were very developed.

Centuries later, the second world war balanced because of a cryptanalysis team hard work at Bletchley park in U.K. They broke Enigma, the famous german encryption machine and got the ability to "read" the confidential messages exchanged within german army. They got the posibility to know e.g. the plans and the positions.

Here is a general classification of cryptanalysis attacks [1]:

2.2.2 Cryptanalysis attacks

cipher-text-only attack

This is the most general attack where the attacker has access only to cipher-text. Since cipher-texts are sent and received via communications mediums (e.g. networks, radio, satellites), one has to suppose the availability, by default, of all cipher-texts to potential attackers. So, this attack should be considered for every cryptographic algorithm assessment and is considered as the basic level for security robustness evaluation.

Known-plain-text attack

In this type of attack, it is assumed that the attacker can get pairs of plain-text-cipher-text. The attack consists of trying to decrypt the cipher-text using information extracted and gathered from pairs of plain-text-cipher-text. Using the information extracted from these pairs, the attacker attempts to decrypt a cipher-text for which he does not have the plain-text. The use of standard formats of messages could be useful to the attacker in conducting known-plain-text attack [1].

Chosen-plain-text attack

In this type of attack, it is assumed that the attacker can encrypt plain-texts of his choice and get their correspnding cipher-texts. Naturally, to realize such an attack, the attacker has to get access, at least, once to the encryption device [1]. Then, the cryptanalysis work consists of trying to decrypt cipher-texts for which he does not have the corresponding plain-text.

Adaptively-chosen-plain-text attack

This type of attack is similar to the chosen plain-text attack except that here, the attacker can get more pairs of plain-text-cipher-text by doing some analysis and can have access as long as he wants to the encryption device [1].

Chosen-and adaptively-chosen-cipher-text attack

In this type of attack, the attacker has the ability to choose cipher-texts and then decrypt them to get the corresponding plain-texts. He needs to have access to the decryption device [1].

Despite the type of the cryptanalysis attack, a basic principle of cryptanalysis is to assume that the algorithm is not secret i.e. it is well known by the attacker.

2.2.3 Non-classical cryptanalysis approach

The robustness of a cryptographic application depends not only on its pure mathematical model but also on its implementation on soft and/or hardware devices. Some parameters which are not involved in the mathematical aspect of cryptographic solutions and, hence, trend to be ignored in the security evaluation such as execution time and power consumption can be very important and reveal secret information. This can cause the break of a, theoretically secure, cryptographic algorithm [22].

"Side channel attacks" are attacks that exploit this side channel information to retrieve the secret information treated by cryptographic devices [22]. Several types of side channel attacks are already published in the litterature. They include timing attacks [24], power analysis attacks [25], electromagnetic attacks [26], fault induction attacks and template attacks [27, 28]. For a cryptographic system to remain secure it is imperative that the secret keys, that it uses to perform the required security services, are not revealed in any way [29].

Where cryptosystems are being used in real applications, not only mathematical attacks have to be taken into account. Hard and software implementations themselves present a vast field of attacks. Side-Channel Attacks

exploit information that leaks from a cryptographic device [25].

2.3 A brief reminder on some basics on linear algebra

This is not a linear algebra section, however it turns out that many important mathematical properties of cryptography and cryptanalysis are based on algebraic concepts [20]. That is why a brief reminder is necessary for eliminating any reader confusion on the cryptographic construction explained in this thesis.

Subspace : The space $\mathcal{H}$ spanned by a collection of vectors $\{\mathbf{x}_k\}$

$$\mathcal{H} := \{\alpha_1\mathbf{x}_1 + \cdots + \alpha_n\mathbf{x}_n | \alpha_i \in \mathbf{C}, \forall i\}$$

is called a *linear subspace*.

Basis : An independent collection of vectors that together span a subspace is called a *basis* for that subspace.
If the vectors are orthogonal ($\mathbf{x}_i{}^H\mathbf{x}_j = 0, i = j$), it is an *orthogonal basis*.

Projection : A square matrix $\mathbf{P}$ is a projection if $\mathbf{PP} = \mathbf{P}$.
It is an orthogonal projection if also $\mathbf{P}^H = \mathbf{P}$.

- The norm of an orthogonal projection is $\|\mathbf{P}\| = 1$.
- For an isometry $\hat{\mathbf{U}}$, the matrix $\mathbf{P} = \hat{\mathbf{U}}\hat{\mathbf{U}}^H$ is an orthogonal projection (onto the space spanned by the columns of $\hat{\mathbf{U}}$).

Notations

T, H, $\sharp$ denote transpose, conjugate-transpose, Moore-Penrose pseudoinverse, respectively. We will denote matrices and vectors with boldface type, using capital letters for matrices and lower-case letters for vectors. Given a matrix $\mathbf{A} \in \mathbb{C}^{N\times r}$, we denote the range subspace of $\mathbb{C}^N$ spanned by the $r \leq N$ columns of $\mathbf{A}$ by $\langle A \rangle$.

2.4 Blind source separation in cryptography

In this section, we presente an overview of the use of blind source separation techniques in the cryptography field.

2.4.1 Blind source separation (BSS) techniques

Let us first start by introducing the blind source separation (BSS). The latter aims to recover a set of unknown mutually independent source signals from their observed mixtures without knowing the mixing coefficients [2, 3]. Suppose that there exists M independent source signals and N observed mixtures of the source signals (usually $M \leq N$). The linear BSS mixing model is as follows:

$$\mathbf{x}(t) = \mathbf{H}\mathbf{s}(t) \tag{2.3}$$

where $\mathbf{s}(t) = [s_1(t), \cdots, s_M(t)]^T$, which is an $M \times 1$ column vector collecting the source signals, vector $\mathbf{x}(t)$ similarly collects the N observed (mixed) signals, and $\mathbf{H}$ is an $N \times M$ mixing matrix that contains the mixing coefficients.

The purpose of BSS is to find an $M \times N$ demixing matrix $\mathbf{W}$ such that the $M \times 1$ output vector $\mathbf{u}(t)$ verifies

$$\mathbf{u}(t) = \mathbf{W}\mathbf{x}(t) = \mathbf{W}\mathbf{H}\mathbf{s}(t) = \mathbf{P}\mathbf{D}\mathbf{s}(t) \tag{2.4}$$

where $\mathbf{P}$ and $\mathbf{D}$ denote a permutation matrix and diagonal matrix, respectively. When $M \leq N$, the blind source separation and more specifically source recovery is possible. However, when $M > N$, BSS becomes generally impossible except under specific conditions [30, 31, 32]. This is referred to as the under-determined BSS problem.

2.4.2 BSS-based encryption

Among cryptographic techniques, Blind Source Separation (BSS)-based methods have received recently some attention in speech and image encryption fields.

In [33], a scheme using BSS techniques is proposed for encryption purpose. A series of encryption schemes based on BSS is introduced [4, 5, 6]. In [4] and [5], the linear mixing model of blind source separation is used

in image encryption. The transmitted images are hidden in a noise image by specific mixing before encryption and then recovered through BSS after decryption [4]. A speech encryption algorithm which integrates a modified time domain scrambling scheme was used to mask the speech signal with a random noise by specific mixing [6]. A speech encryption scheme is presented in [7] by taking advantage of the underdetermined BSS problem to construct the mixing matrix for encrypting multiple segments simultaneously and enhancing the security level of the previous schemes.

In [7], the encryption procedure, including the use of key signals, has been represented as:

$$\mathbf{x}(t) = \mathbf{A}_p\mathbf{p}(t) + \mathbf{A}_k\mathbf{k}(t) \tag{2.5}$$

where $\mathbf{p}(t) = [p_1(t), \cdots, p_M(t)]^T$ and $\mathbf{k}(t) = [k_1(t), \cdots, k_M(t)]^T$ represent M input plain-signals and M key signals, respectively. $\mathbf{A}_p$ and $\mathbf{A}_k$ are $M \times M$ matrices, both of which elements are within $[-1, 1]$. The decryption procedure, as long as $\mathbf{A}_s$ is invertible, is given by:

$$\mathbf{p}(t) = \mathbf{A}_p^{-1}\ (\mathbf{x}(t) - \mathbf{A}_k\mathbf{k}(t)). \tag{2.6}$$

In the BSS-based encryption scheme [7], the key signals $k_1(t), \cdots, k_M(t)$ are as long as the plain-signals and have to be generated by a pseudo-random number generator (PRNG) with a secret seed, which serves as the secret key. The mixing matrices $\mathbf{A}_s$ and $\mathbf{A}_k$, being secret parameters, may be known by the receiver as secret keys and hence their estimation by a BSS approach at the receiver should not be necessary. Hence, the BSS approach is, in this case, worth to be used in a cryptanalysis process rather than in an encryption one.

However, some weaknesses from a cryptographic point of view exist and the security against some attacks is not sufficiently strong.The encryption procedure described in equation (2.5) could be presented under the form of two steps [11]:

- *Step 1:* $\mathbf{x}^{(1)}(t) = \mathbf{A}_p\ \mathbf{p}(t)$*;*
- Step 2: $\mathbf{x}(t) = \mathbf{x}^{(1)}(t) + \mathbf{A}_k\mathbf{k}(t)$.

As it is presented above, one can see that this procedure is equivalent to a simple matrix-based block cipher in the first step and a simple-addition based stream cipher. The security of this BSS-based encrytpion scheme is analyzed in the following section.

2.4.3 Cryptanalysis of BSS-based encryption

In this section, security weaknesses and defects of BSS-based encryption scheme are discussed especially its weaknesses against known/chosen-palintext attack and chosen-cipher-text attack [11].

The mixing matrix A

As long as the principles of BSS techniques are respected, the mixing matrix $\mathbf{A}$ seems to be not required at the decryption side to separate the encrypted signals [11]. However, if it is so, i.e. $\mathbf{A}$ is not a secret parameter and considering that $\mathbf{x}^*(t) = \mathbf{A}_p^{-1}\mathbf{x}(t)$ is the equivalent obtained encrypted-signal to the encryption procedure described by equation (2.5), the encryption procedure could hence be given by:

$$\mathbf{x}^*(t) = \mathbf{p}(t) + \mathbf{A}_p^{-1}\mathbf{A}_k(t) \tag{2.7}$$

As it is shown in the the encryption procedure given by equation (2.7), there is no underdetermined BSS problem [11].

On another hand, if the mixing matrix $\mathbf{A}$ is not a secret parameter, the BSS-based encryption scheme would be in front of the problem of closely-related input signals as it is the case in an image and its watermarked version. This difficulty is due to an essential hypothesis in BSS systems: the input signals are mutually independent of each other. Thus, it is clear that the mixing matrix $\mathbf{A}$ must be part of secret parameter used in BSS encryption scheme [11].

How key space is large?

A mixing matrix $\mathbf{A}$ of dimension $P \times Q$, the secret key parameter of BSS-based encryption scheme, has the interval [-1,1] for all its elements [4]-[10]. So, the number of all possible mixing matrix $\mathbf{A}$ is $R^{(P+Q)}$ where R is determined by the finite precision under which the cryptosystem is realized. P and Q are the number of input plain-signals and the number of key signals, respectively. Note that the BSS-based encryption scheme is mainly based on the principle of creating an underdetermined case by constructing a vector which contains both the plain-signals and the key signals. This gives arise to a $(P + Q)$ cipher-signals and leads to a $R^{(P+Q)}$ possible mixing matrices. For example, if the cryptosystem is implemented with n-bits fixed-point arithmetic,

$R = 2^n$; if it is implemented with $IEEE$ floating-point arithmetic, $R = 2^{31}$ (single-precision) or $R = 2^{63}$ (double-precision) [11, 34].

Furthermore, the key signals $\mathbf{k}(t)$ are generated using a Pseudo Random Number Generator (PRNG) with a key seed $\mathbf{I}_0$ which has a length of J bits. This means that the size of the key space of key signals $\mathbf{k}(t)$ is 2^J. Thus, the size of the whole key space of the BSS-based encryption scheme is $R^{P(P+Q)}2^J$. In the case where $\mathbf{A} = [\mathbf{B}, \beta\mathbf{B}]$, the size of the key space is $R^{P^2}2^J$ [11].

Divide-and-Conquer (DAC) Attack

The encryption procedure described in equation (2.5) could be rewritten as:

$$\mathbf{p}(t) \;=\; \hat{\mathbf{A}}\ \mathbf{x}_k(t) \tag{2.8}$$

where $\mathbf{x}_k(t) = [x_1(t), \cdots, x_P(t), k_1(t), \cdots, k_Q(t)]^T$ and

$$\hat{\mathbf{A}} = \mathbf{A}_p^{-1}\ [\mathbf{I}, -\mathbf{A}_k] \;=\; [\mathbf{A}_p^{-1}, -\mathbf{A}_p^{-1}\mathbf{A}_k]$$

As it can be seen from the above equation, the knowledge of $\mathbf{k}(t)$ and the i-th row of $\hat{\mathbf{A}}$ allows recovering $p_i(t)$. This means that a divide-and-conquer attack (DAC) could separately break P rows of $\hat{\mathbf{A}}$. Hence, the number of possible mixing matrices becomes $PR^{(P+Q)}$ rather than $R^{P(P+Q)}$. Consequently, the size of the whole key space will be $PR^{(P+Q)}2^J$ rather than $R^{P(P+Q)}2^J$ [11].

Sensitivity to the mixing matrix A

A good cryptosystem should have a high sensitivity to key mismatch. This means that if two slightly different encryption keys are used to encrypt the same plain-text, the obtained cipher-texts should be very different [11, 17]. In the BSS encryption scheme, considering two mixing matrices $\mathbf{A}_1 = [a_{1;i,j}]$ and $\mathbf{A}_2 = [a_{2;i,j}]$ of size M x N, if ϵ is the maximal difference of all elements, then Δx_i, the i-th element of $\Delta\mathbf{x}$ is given by:

$$\Delta\mathbf{x} = \mathbf{A}_1\mathbf{p}(t) - \mathbf{A}_2\mathbf{p}(t)$$

One can see that $\Delta\mathbf{x}$ verifies the following inequality:

$$\begin{aligned} |\Delta x_i| &= |\sum_{j=1}^{N}(a_{1;i,j} - a_{2;i,j})p_j| \\ &\leq \sum_{j=1}^{N}|a_{1;i,j} - a_{2;i,j}|.|p_j| \\ &\leq N\epsilon \max(|\mathbf{p}(t)|) \end{aligned} \tag{2.9}$$

where $|\mathbf{p}(t)|$ is the vector which contains absolute values of all elements of $\mathbf{p}(t)$, i.e., $|\mathbf{p}(t)| = [\ |p_1(t)|\ ...\ |p_N(t)|\ ]^T$. The mixing matrix can be approxiamtely guessed under a relatively large finite precision ϵ [11].

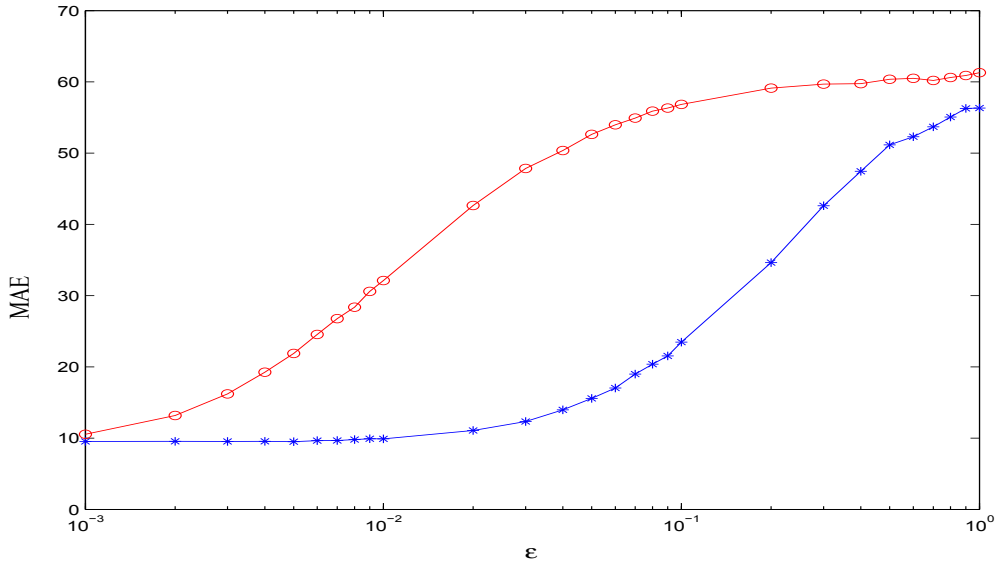
This low sensitivity of BSS-based encryption scheme to the mixing matrix is verified by the results obtained from encrypting a plain-text $\mathbf{p}(t)$ using a mixing matrix $\mathbf{A}$ and decrypting the resulting cipher-text $\mathbf{x}(t)$ using a mismatched mixing matrix $(\mathbf{A}, \epsilon\mathbf{R})$ where $\epsilon \in [0, 1]$ and $\mathbf{R}$ is a $P\times(P+Q)$. After decryption, one gets $\hat{\mathbf{p}}(t)$ which is an estimated version of $\mathbf{p}(t)$. The exhaustively search for an approximate version of the mixing matrix $\mathbf{A}$ under the finite precision ϵ 0.01 allows to get a good estimation of the plain-texts [11].

Figure (2.1) shows the experimental relationship in the BSS-based encryption scheme between the recovery error and the value of ϵ for respectively a digital image and a speech signal. Beside the fact that experimental results confirm that a plain-text can be approximately recovered by a mismatched key, humans have a good capability of distinguishing images and speechs even in presence of errors [11].

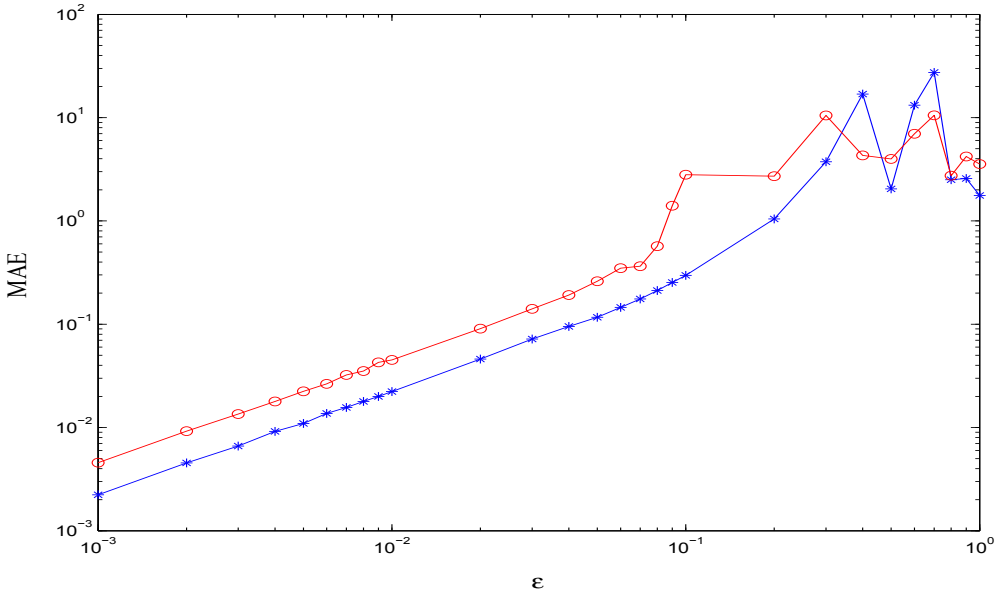
Figure (2.2) shows a recovered plain-speech resulting from an exhaustively search of the mixing matrix $\mathbf{A}$ with a relatively large value of $\epsilon = 0.1$.

Sensitivity to the key signals $\mathbf{k}(t)$

The BSS-based encryption scheme has a low sensitivity to key signals mismatch because of the same reason of its low sensitivity to mixing matrix mismatch. If the maximal difference of all elements of two key signals $\mathbf{k}_1(t)$ and $\mathbf{k}_2(t)$ is ϵ, then each element of $|\mathbf{A}_k\mathbf{k}_1(t) - \mathbf{A}_k\mathbf{k}_2(t)|$ is not greater than $Q\ \max(|\mathbf{A}_k|)\epsilon = Q\epsilon$.



(a)



(b)

Figure 2.1: The experimental relationship between the recovery error and the value of ϵ in BSS encryption system for, (a) the plain-text is an image, (b) the plain-text is a speech signal

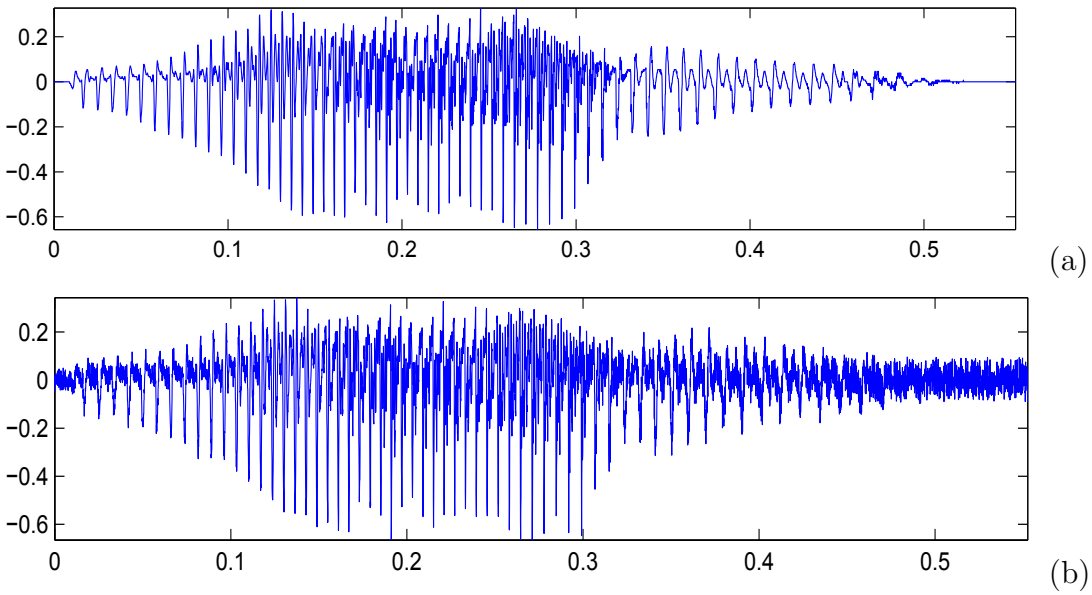


Figure 2.2: A recovered speech from an exhaustively search of the mixing matrix $\mathbf{A}$ when $P = 2$ and $\mathbf{A} = [\mathbf{B}, \mathbf{B}]$: (a) the original plain-speech; (b) the recovered speech

Differential attack

The differential $\Delta_{\mathbf{x}}(t)$ between two cipher-texts $\mathbf{x}^{(1)}(t)$ and $\mathbf{x}^{(2)}(t)$ obtained from encrypting two plain-texts $\mathbf{p}^{(1)}(t)$ and $\mathbf{p}^{(2)}(t)$ using the same encryption key $(\mathbf{A}, \mathbf{I}_0)$ is given by:

$$\Delta_{\mathbf{x}}(t) = \mathbf{A}_p^{-1}\Delta_{\mathbf{p}}(t) \tag{2.10}$$

where $\Delta_{\mathbf{x}}(t) = \mathbf{x}^{(1)}(t) - \mathbf{x}^{(2)}(t)$ and $\Delta_{\mathbf{p}}(t) = \mathbf{p}^{(1)}(t) - \mathbf{p}^{(2)}(t)$. Due to the low sensitivity of BSS-based encryption scheme to mixing matrix $\mathbf{A}$ (as it is shown in Sec. (2.4.3), an exhaustive search could be applied to recover $\mathbf{A}_p$ [11]:

$$\Delta_{\mathbf{p}}(t) = \mathbf{A}_p^{-1}\Delta_{\mathbf{x}}(t) \tag{2.11}$$

In fact, the effect of key signals $\mathbf{k}(t)$ does not exist anymore when a differential attack is applied. Then, a mixed view of two interested plain-texts is obtained from the above calculation of the plain-text difference.

Low sensitivity to plain-text

In a good cryptosystem, the encryption of two plain-texts with a very slight difference should be very different [11]. However, in the BSS-based encryption scheme, when we use two very close plain-texts $\mathbf{p}_1(t)$ and $\mathbf{p}_2(t)$ for which the maximal difference of all elements is ϵ, then each element of $|\mathbf{A}_p\mathbf{p}_1(t) - \mathbf{A}_p\mathbf{p}_2(t)|$ is not greater than P max $(|\mathbf{A}_p|)\epsilon = P \times \epsilon$. This low sensitivity increases when the two plain-texts are closely correlated as in the case of a plain-text and its watermarked version [11].

Known-plain-text attack

By encrypting plain-texts with the same key, one can get in this type of attack plain-text differences . From equation (2.10), the mixing matrix can be determined using P plain-text differences as follows:

$$\mathbf{A}_p = \Delta_{\mathbf{x}}(t)(\Delta_{\mathbf{p}}(t))^{-1} \tag{2.12}$$

where $\Delta_{\mathbf{p}}(t)$ and $\Delta_{\mathbf{x}}(t)$ are $P \times P$ matrices, constructed row by row from the P plaint-texts and the corresponding cipher-texts differences, respectively. Considering that n dstinct plain-texts can generate $n(n-1)/2$ plain-text

differences [11]. The number n of required plain-texts to yield at least P plain-text differences is given by $n \geq \sqrt{P}$ after solving the inequality:

$$n \geq \lceil \sqrt{P - 1/4} + 1/2 \rceil \approx \sqrt{P} \tag{2.13}$$

Chosen plain-text/cipher-text attack

With a slight difference, the chosen-plain-text attack and the differential known-plain-text attack applied on BSS-based encryption scheme give roughly the same result [11]. In the chosen-cipher-text attack, one can choose a number of cipher-texts and observe the corresponding plain-texts.

2.4.4 Conclusion on cryptanalysis of BSS-based encryption scheme

The security robustness of BSS-based encryption scheme is evaluated. The cryptanalysis robustness study considers the cipher-text-only attack approach in terms of the resistance level to divide-and-conquer (DAC) attack and to differential attack, as well as the evaluation of sensitivity to the mixing matrix, to the key signals and to the plain-text. In known-plain-text attack approach, the number of required plain-texts to yield at least P plain-text differentials has been evaluated [11].

At this level, the analysis of the security robustness of BSS-based encryption scheme has shown that, in the actual architecture of this system, some weaknesses, from a crptographic point of view, still exist. First, the key signals $\mathbf{k}(t)$ do not play any important security role in the case of a differential attack. This means that the effect of the second term of the encryption procedure described in equation (2.5) is cancelled. Second, the use of the mixing matrix several times beside the low sensitivity of encryption/decryption constitute a weakness of BSS-based encryption scheme.

However, from another point of view, in the BSS-based encryption scheme, the low sensitivity of decryption to cipher-text could be seen as an advantage in the case of the need to lossy decryption. Lossy decryption means that even when the receiver gets a cipher-text which is slightly different from the requetsed one, the decryption process could be achieved successfully. The lossy decryption is usefull in some real applications where the cipher-text could be

compressed with some lossy algorithms to save the required storage. But, from a cryptographic point of view, this feature constitutes a considerable weakness [11].

Chapter 3

Orthogonal Subspace-based Encryption

In this chapter, we take advantage from the security defects of BSS-based encryption scheme revealed by the cryptanalysis attacks to propose a new encryption scheme based on subspace concept. The first approach is based on orthogonal subspace concept. The design of such a system mainly consists of the optimization of the following attributes:

- Crytpographic robustness based essentially on confusion and diffusion principles.
- Quality of restitution of the original signal after decryption.

3.1 Subspace-based Encryption

The two main steps in an encryption scheme are the encryption and the decryption steps. In practice, the output of the encryption step is transmitted through a communication channel then received at the receiver hand before being processed in the decryption step. For simulation purposes, we consider that the communication channel is ideal and hence, the output of the encryption step is actually the input of the decryption step.

3.1.1 Encryption

The block diagram of the proposed encryption scheme is shown in Figure (3.1). The data are first fed to the segment splitter which consists of

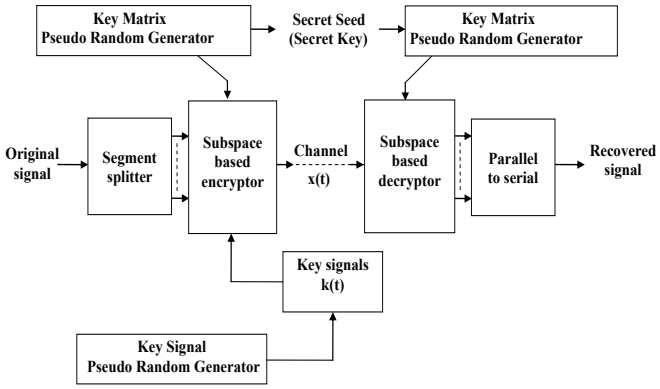


Figure 3.1: Block diagram of the proposed orthogonal subspace-based encryption.

dividing the original signal into L segments:

$$\mathbf{p}(t) = [p_1(t), \cdots, p_M(t)]^T, \ t = 1, \cdots, L \tag{3.1}$$

where M is the segment length. The plain signal contains $L \times M$ samples, it is split in L segments of M samples, the M samples form the $M \times 1$ vector $\mathbf{p}(t)$ of equation (3.2). Hence, L is the number of segments. It becomes the sample size of the vector $\mathbf{x}(t)$ of equation (3.2). These segments are used in the encryption process (the subspace-based encryption block) to obtain the following encrypted signal:

$$\mathbf{x}(t) = \mathbf{A}(t)\mathbf{p}(t) + \beta \mathbf{P}^{\perp}_{A(t)} \mathbf{B}(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{p}(t))] \tag{3.2}$$

where $\mathbf{A}(t)$ and $\mathbf{B}(t)$ are $(M+1) \times M$ and $(M+1) \times M$ full rank key matrices, respectively. The introduction of matrices $\mathbf{A}(t)$ and $\mathbf{B}(t)$ is motivated by the task of increasing the key space that would be needed for cryptanalysis. Note that the key matrices are generated for each vector $\mathbf{x}(t)$. This property makes any estimation of the signal subspace impossible from only

one snapshot. These matrices can be generated by a pseudo-random number generator (PRNG) with a secret seed that serves as the secret key.

β is a factor that controls the signal to noise ratio. This factor (β) should be chosen as large as possible in order to provide very low Signal to Noise Ration (SNR), $\mathbf{g}(.)$ is a component-wise nonlinear function that verifies

$$\mathbf{g}(0) = 0. \tag{3.3}$$

$\mathbf{k}(t)$ is a random $M \times 1$ key signal vector generated by any robust key signal generator and $\odot$ denotes the Hadamard operator. $\mathbf{P}^{\perp}_{A(t)}$ is the projector on the orthogonal subspace to the one spanned by the columns of the key matrix $\mathbf{A}(t)$. The latter is refereed herein to as the key subspace. The projector $\mathbf{P}^{\perp}_{A(t)}$ is given by

$$\mathbf{P}^{\perp}_{A(t)} = \mathbf{I} - \mathbf{P}_{A(t)} = \mathbf{I} - \mathbf{A}(t)(\mathbf{A}(t)^H\mathbf{A}(t))^{-1}\mathbf{A}(t)^H \tag{3.4}$$

where $\mathbf{P}_{A(t)}$ is the orthogonal projector on the key subspace, and $(.)^H$ and $\mathbf{I}$ denote the Hermitian operator and the identity matrix, respectively. For the purpose of robustness evaluation, we use in the sequel the following component-wise nonlinear function:

$$g(v) = \frac{v}{\sqrt{1+v^2}} \tag{3.5}$$

that verifies condition (3.3).

3.1.2 Decryption

On the receiver hand, the encrypted data vector is first projected on the corresponding key subspace; this is done by the following operation:

$$\mathbf{x}_p(t) = \mathbf{P}_{A(t)}\mathbf{x}(t) \tag{3.6}$$

where $\mathbf{x}_p(t)$ is the obtained projected data. Since the projectors $\mathbf{P}_{A(t)}$ and $\mathbf{P}^{\perp}_{A(t)}$ are orthogonal (i.e. $\mathbf{P}_{A(t)}\mathbf{P}^{\perp}_{A(t)} = \mathbf{0}$), the above projection leads to the following result

$$\mathbf{x}_p(t) = \mathbf{A}(t)\mathbf{p}(t) \tag{3.7}$$

and the original plain-text (the decrypted signal) is obtained by using the key matrice $\mathbf{A}(t)$:

$$\mathbf{p}(t) = (\mathbf{A}(t))^{\sharp}\mathbf{x}_p(t) \tag{3.8}$$

where $(.)^{\sharp}$ denotes the pseudo-inverse operator.

Note that in the above recovery procedure, one does not need to know the key signals $\mathbf{k}(t)$ neither the matrix $\mathbf{B}(t)$.

The $\mathbf{k}(t)$ in equation (3.2) is not the same as that used in the blind source separation-based encryption scheme. The difference is in the way of its use. In blind source separation-based encryption scheme, $\mathbf{k}(t)$ is included in the transmitted source vector in order to generate an under-determined blind source separation source (BSS) problem.

In our proposed method, $\mathbf{k}(t)$ is used with conjoncture with a non-linearity of the data as an additive perturbation term that also generate an under-determined blind source separation source(BSS) problem. The dimension of $\mathbf{k}(t)$ is $M \times 1$. $\mathbf{k}(t)$ is generated by any pseudo random or random generator. There is no specific range for values of $k(t)$. It depends on the chosen key generator.

Of course, the randomness quality of the key signals of any encryption system can affect the encryption results. In our case, this is also true. However, the randomness quality is guaranteed by the pseudo random or random generator used in the encryption system (see [35]-[38]) .

For simplicity, the Matlab generic instruction "random" has been used. Several pseudo random and random generators exist, both in software and hardware forms, and any generator which fulfills the randomness criteria largely described in the literature (e.g. NIST tests of randomness, Maurer test) [39, 40] can be used to generate $\mathbf{k}(t)$. However, the issue of studying and evaluating the randomness of the key generators, both pseudo random and random, is over the scope of this thesis.

Currently, the factor β in equation (3.2) should be chosen as large as possible in order to provide very low SNR. For such chosen values that should lead to secure encrypted data, we can not get small eigenvalues for this subspace.

If one set $\beta = 0$, this means that we have no encryption according to the proposed scheme. Even if one can estimate $\mathbf{A}$ from the encrypted data $\mathbf{x}$, the estimate $\hat{\mathbf{A}}$ will be given with some estimation error say $\Delta\mathbf{A}$:

$$\hat{\mathbf{A}} = \mathbf{A} + \Delta\mathbf{A}$$

Note that the existing correlation between the two terms of equation (3.2) will increase the estimation error if one find a way to estimate $\mathbf{A}$ or its subspace. Beside this property, several tests have been conducted to measure the sensitivity of the proposed scheme even to very small matrix mismatch. Results of these tests are presented in chapter 6.

3.2 Iterative Orthogonal Subspace-based Encryption

The iteration of an encryption scheme for a number of rounds is usually applied on cryptosystems to enhance their security characteristics and hence, strengthen their resistance to cryptanalysis attacks. At this level, our proposed subspace-based encryption scheme described in section (3.1) constitutes one round. The output of the first round is re-injected as the input for the second round and so on. The output of the last round represents the output of the whole encryption scheme i.e. the iterative subspace-based encryption scheme. Figure (3.2) shows the block diagram of the proposed iterative subspace-based encryption scheme.

3.2.1 Encryption

The splitted segments of equation (3.1) are used in the iterative encryption process to obtain the following encrypted signal:

$$\mathbf{x}_n(t) = \mathbf{A}_n(t)\mathbf{x}_{(n-1)}(t) + \beta\mathbf{P}^{\perp}_{A_n(t)}\mathbf{B}_n(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{x}_{(n-1)}(t))] \tag{3.9}$$

where $\mathbf{x}_n(t)$ and $\mathbf{x}_{(n-1)}(t)$ denote the n^{th} and $(n-1)^{th}$ encrypted segments. $n \geq 1$ and $\mathbf{x}(0)$= $\mathbf{p}(t)$, the plain-text. $\mathbf{A}_n(t)$ and $\mathbf{B}_n(t)$ are $(M+1) \times M$ full rank key matrices, respectively. Note that the encryption process described in equation (3.9) is performed on several iterations.

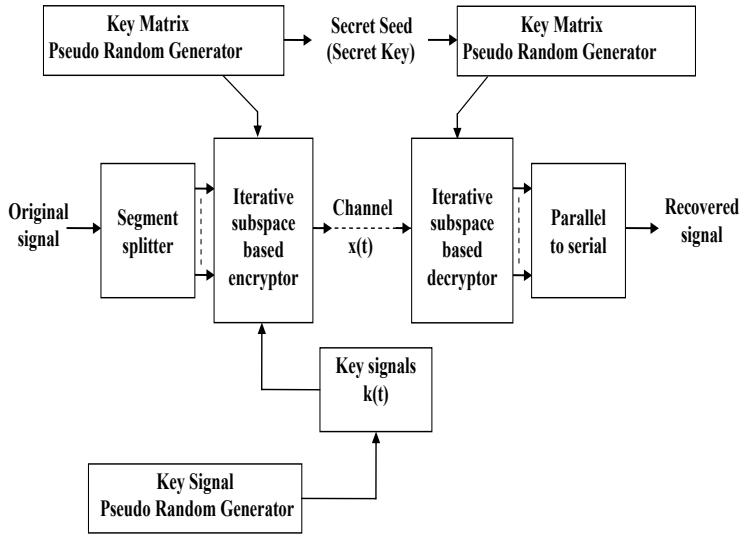


Figure 3.2: Block diagram of the iterative subspace-based encryption.

3.2.2 Decryption

Once the cipher-text is obtained, the decryption procedure could be achieved by projecting the last encrypted segment $\mathbf{x}_{n(t)}$ as described by the following equation:

$$\mathbf{x}_{p,n}(t) = \mathbf{P}_{A_n(t)}\mathbf{x}_{n(t)} \tag{3.10}$$

where $\mathbf{x}_{p,n}(t)$ is the obtained projected data. Since the projectors $\mathbf{P}_{A_n(t)}$ and $\mathbf{P}^{\perp}_{A_n(t)}$ are orthogonal (i.e. $\mathbf{P}_{A_n(t)}\mathbf{P}^{\perp}_{A_n(t)} = \mathbf{0}$), the above projection leads to the following result:

$$\mathbf{x}_{p,n}(t) = \mathbf{A}_n(t)\mathbf{x}_{(n-1)}(t) \tag{3.11}$$

The decrypted signal at iteration $n-1$, is then obtained by

$$\mathbf{x}_{(n-1)}(t) = (\mathbf{A}_n(t))^{\sharp}\mathbf{x}_{p,n}(t) \tag{3.12}$$

where $(.)^{\sharp}$ denotes the pseudo-inverse operator. The above equations are performed iteratively till restituting the original plain-text.

3.3 Conclusion

In this chapter, an orthogonal subspace-based encryption scheme is presented. Characteristics of this scheme, from a security point of view, are described. First, the key matrix $\mathbf{A}$ is generated for each segment of the plain-text which means that there are as many key matrices as segments of plain-text. Second, the key signals $\mathbf{k}(t)$ used during the encryption step are no longer necessary for achieving decryption at the receiver side. Third, a nonlinearity is guaranteed in this system through the use of a component-wise nonlinear function. Fourth, in the absence of a plain-text at the input of the proposed encryption scheme, there is no output at the receiver side i.e. there is no cipher-text. Fifth, a correlation is achieved between the various components of the encryption procedure.

Furthermore, the iterative orthogonal subspace-based encryption approach, through the process of applying the encryption for several rounds, provides an added value in the sense that it allows to acuumulate characteristics which are already guaranteed by the one-round orthogonal system. Of course, the application of several rounds in the iterative orthogonal subspace-based encryption scheme has a cost in terms of processing speed and consequently time of execution. A compromise, depending on the requirements of the target field of application of the subspace-based encryption scheme, has to be found between number of iterations and processing speed. This issue becomes more important when a hardware implementation is considered.

Chapter 4

Oblique Subspace-based Encryption

In this chapter, we propose an encryption scheme based on oblique subspace concept rather than orthogonal subspace concept as described previously in chapter (3). The differences between the two approaches are shown and a conclusion on the added value of the oblique subspace-based approach is given. As it is mentioned in section (3.1), the output of the oblique subspace-based encryption and the input of the oblique subspace decryption are the same. For clarity, a brief review of oblique projection is given in the following section.

4.1 Oblique Projection

Let us recall the following notations, we denote the orthogonal projection on range subspace $\langle A \rangle$ by $\mathbf{P_A}$, and the orthogonal projection on range space orthogonal to $\langle A \rangle$ by $\mathbf{P_A^\perp} = \mathbf{I} - \mathbf{P_A}$.

The oblique projection matrix on one range of the subspace $\langle A \rangle$ obliquely to the null subspace $\langle B \rangle$ is defined by:

$$\mathbf{E}_{AB} = \mathbf{A}(\mathbf{A}^H \mathbf{P}_B^\perp \mathbf{A})^{-1} \mathbf{A}^H \mathbf{P}_B^\perp \tag{4.1}$$

and

$$\mathbf{E}_{BA} = \mathbf{P}_B(\mathbf{I} - \mathbf{E}_{AB}) \tag{4.2}$$

4.1.1 Properties

The matrix $\mathbf{E}_{AB}$ is idempotent, but not symmetric, and has the following properties [41]:

- Range subspace $\langle A \rangle$ and null subspace $\langle B \rangle$:

$$\mathbf{E}_{AB}\mathbf{A} = \mathbf{A}, \mathbf{E}_{AB}\mathbf{B} = 0 \tag{4.3}$$

- The two matrices decompose the projection $\mathbf{P_{AB}}$ as follows:

$$\mathbf{P_{AB}} = \mathbf{E}_{AB} + \mathbf{E}_{BA} \tag{4.4}$$

- The oblique projection operator is invariant to change of basis [42].

Next, this concept of Oblique Projection is exploited to improve our proposed subspace-based encryption.

4.2 Encryption System based on Oblique Projection

As it was mentioned in section (3.1), we consider that the communication channel is ideal and then, the output of the encryption step is exacly the input of the decryption step. These two main steps in an encryption scheme will be explained in the following sections.

4.2.1 Encryption

The main difference between the block diagram of the proposed oblique subspace-based encryption scheme shown in Figure (4.1) and the block diagram shown in Figure (3.1) is in the subspace-based encryptor i.e. the subspace-based encryptor shown in Figure (4.1) is an oblique subspace-based encryptor rather than an orthogonal one.

The plain-text is first divided into L segments before being fed to the oblique subspace-based encryptor to give arise to the following cipher-text (encrypted signal):

$$\mathbf{x}(t) = \mathbf{A}(t)\mathbf{p}(t) + \beta\mathbf{B}(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{p}(t))] \tag{4.5}$$

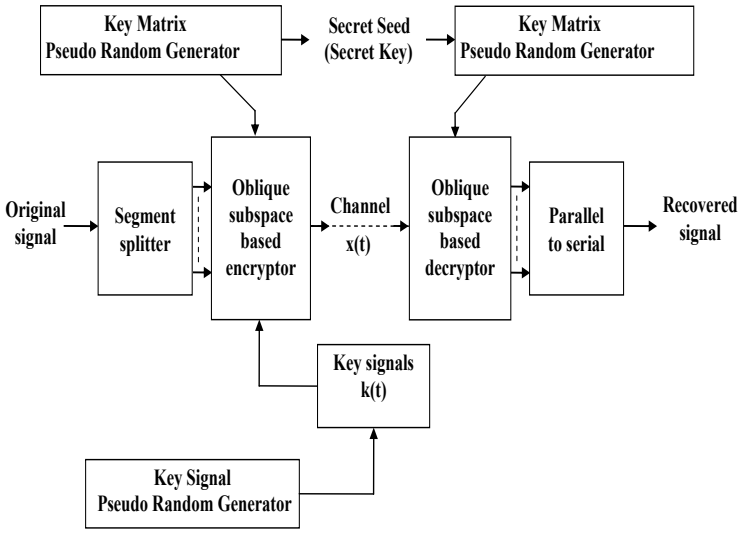


Figure 4.1: Block diagram of the oblique subspace-based encryption.

where $\mathbf{A}(t)$ and $\mathbf{B}(t)$ are $(M+1)\times M$ and $(M+1)\times 1$ full rank key matrices, respectively.

Note that the key matrices are also, as it is the case in the orthogonal subspace-based encryption, generated for each vector $\mathbf{x}(t)$.
β is a factor that controls the signal to noise ratio and $\mathbf{g}(.)$ is a component-wise nonlinear function that verifies the same condition required for the orthogonal subspace-based encryption i.e.

$$\mathbf{g}(0) = 0$$

$\mathbf{k}(t)$ is a random $M \times 1$ key signal vector generated by any robust key signal generator and $\odot$ denotes the Hadamard operator. For the purpose of robustness evaluation, we use in the sequel the same component-wise nonlinear function:

$$g(v) = \frac{v}{\sqrt{1+v^2}}$$

that verifies condition (4.6).

4.2.2 Decryption

To achieve decryption, the encrypted data vector received is first projected as it is described in the following equation:

$$\mathbf{x}_p(t) = \mathbf{E}_{A(t)B(t)}\mathbf{x}(t) \tag{4.6}$$

where $\mathbf{x}_p(t)$ is the obtained projected data on the range subspace $\langle A(t)\rangle$ obliquely to the null subspace $\langle B(t)\rangle$.

Since we have:

$$\mathbf{E}_{A(t)B(t)}\mathbf{A(t)} = \mathbf{A(t)}$$

and

$$\mathbf{E}_{A(t)B(t)}\mathbf{B(t)} = 0$$

the above projection leads to the following result:

$$\mathbf{x}_p(t) = \mathbf{A}(t)\mathbf{p}(t) \tag{4.7}$$

and the original plain-text (the decrypted signal) is obtained by using the key matrix $\mathbf{A}(t)$:

$$\mathbf{p}(t) = (\mathbf{A}(t))^{\sharp}\mathbf{x}_p(t) \tag{4.8}$$

where $(.)^{\sharp}$ denotes the pseudo-inverse operator.

As it is shown above, there is no need to have, at the receiver side, the key signals $\mathbf{k}(t)$ neither the matrix $\mathbf{B}(t)$.

The factor (β) should be chosen as large as possible in order to provide very low SNR. For such chosen values that should lead to secure encrypted data, we can not get small eigenvalues for this subspace. As it is mentioned for the orthogonal subspace-based encryption scheme, the existing correlation between the two terms of oblique subspace encryption formula will increase the estimation error if one find a way to estimate $\mathbf{A}$ or its subspace. Several experiments have been conducted to assess the security robustness of the proposed oblique subspace encryption scheme. Results of these tests are presented in chapter 6.

4.3 Iterative Oblique Subspace-based Encryption

Following the same methodology adopted in the iterative orthogonal subspace-based encryption, the oblique subspace-based encryption described in section (4.2) constitutes one round in the iterative oblique subspace-based encryption scheme. The other rounds are comparable to the first one and follow the same procedure except in the input and the output parameters. This means that, for encryption purpose, the input of the second round is exactly the output of the first round and so on. At the end of the encryption process, let us say after n rounds, the output of the n^{th} round is the output of the whole iterative oblique subspace encryption scheme. Figure (4.2) shows the block diagram of the proposed iterative oblique subspace-based encryption scheme.

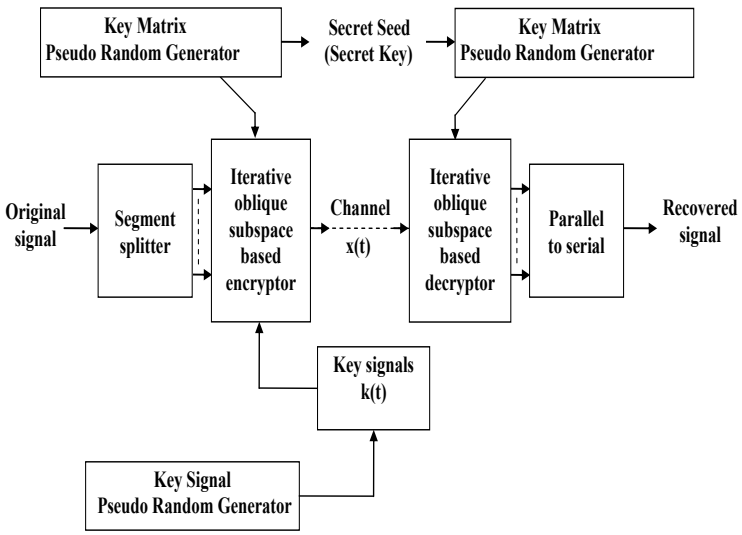


Figure 4.2: Block diagram of the iterative oblique subspace-based encryption.

4.3.1 Encryption

In the iterative oblique subspace-based encryption scheme, the splitted segments described in equation (3.1) are fed to the sytem to get the following encrypted signal:

$$\mathbf{x}_n(t) = \mathbf{A}_n(t)\mathbf{x}_{(n-1)}(t) + \beta\mathbf{B}_n(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{x}_{(n-1)}(t))] \tag{4.9}$$

where $\mathbf{x}_n(t)$ and $\mathbf{x}_{(n-1)}(t)$ denote the n^{th} and $(n-1)^{th}$ encrypted segments. $n \geq 1$ and $\mathbf{x}(0)$= $\mathbf{p}(t)$, the plain-text. $\mathbf{A}_n(t)$ and $\mathbf{B}_n(t)$ are $(M+1) \times M$ and $(M+1) \times 1$ full rank key matrices, respectively. Note that the encryption process described in equation (4.9) is performed on several iterations.

4.3.2 Decryption

The decryption procedure of the received cipher-text could be achieved by projecting the last encrypted segment $\mathbf{x}_{n(t)}$ as described by the following equation:

$$\mathbf{x}_{p,n}(t) = \mathbf{E}_{A_n(t)B_n(t)}\mathbf{x}_{n(t)} \tag{4.10}$$

where $\mathbf{x}_{p,n}(t)$ is the obtained projected data on the range subspace $\langle A_n(t)\rangle$ obliquely to the null subspace $\langle B_n(t)\rangle$.

Since we have:

$$\mathbf{E}_{A_n(t)B_n(t)}\mathbf{A}_n(t) = \mathbf{A}_n(t)$$

and

$$\mathbf{E}_{A_n(t)B_n(t)}\mathbf{B}_n(t) = 0$$

the above projection leads to the following result:

$$\mathbf{x}_{p,n}(t) = \mathbf{A}_n(t)\mathbf{x}_{(n-1)}(t) \tag{4.13}$$

The decrypted signal at iteration $n-1$, is then obtained by

$$\mathbf{x}_{(n-1)}(t) = (\mathbf{A}_n(t))^{\sharp}\mathbf{x}_{p,n}(t) \tag{4.14}$$

where $(.)^{\sharp}$ denotes the pseudo-inverse operator. The above equations are performed iteratively till restituting the original plain-text.

4.4 Conclusion

Through this chapter, we see that the oblique subspace-based encryption scheme is a more general scheme than the orthogonal one in the sense where this later is a specific case of the oblique one.

Characteristics of this scheme, from a cryptographic point of view, as mentioned in section (3.3), are the generation of key matrix for each segment of plain-text, the no-need to the key signals $\mathbf{k}(t)$ used during the encryption step in the decryption procedure, the nonlinearity brought by the use of a component-wise nonlinear function, the cipher-text vanishes if there is no plain-text at the input of the encryption scheme and the correlation between the various elements of the encryption procedure. Furthermore, the iterative oblique subspace-based encryption approach provides an enhancement of these characteristics through the processs of several rounds.

On the other hand, the enhancement provided by the oblique approach, in comparison with the orthogonal approach, consists of making the task of the cryptanalyst more complicated since for the orthogonal subspace-based approach, the knowledge of one subspace leads automaically to the knowledge of the other subspace (the orthogonal one), while in the oblique subspace-based approach, both range subspaces $\langle A \rangle$ and $\langle B \rangle$ should be guessed and hence increases the dimension of the search space.

Chapter 5

Cryptographic Robustness of the Subspace-based Encryption Systems

In this chapter, the proposed subspace-based encryption schemes, orthogonal and oblique, are evaluated to assess their robustness, from a cryptographic point of view, and their quality of recovering the original signal (plain-text). The cryptographic robustness assessment approach is cryptanalysis-oriented in the sense that cryptanalysis attacks are applied on the proposed subspace-based encryption schemes. Results of these cryptanalysis attacks are used to make a comparison with the BSS-based encryption scheme.

5.1 Interpretation of the Subspace-based Encryption in terms of Confusion and Diffusion requirements

In the design of most published cryptographic systems, two important principles are present in the designer's mind: Confusion and Diffusion. Confusion is based on the idea of obscuring the relationship between plain-text, cipher-text and keys. This is done by mixing linearity and nonlinearity [43].

Diffusion is the other important principle of cryptographic system design and is based on the idea that every bit of the cipher-text should depend

on every bit of the plain-text and every bit of the key. This ensures that the statistics of the plain-text are dissipated within the cipher-text so that an attacker cannot predict the plain-text that corresponds to a particular cipher-text, even after observing a number of "similar" plain-texts and their corresponding cipher-texts [43].

Generally, in most of the published cryptographic systems, substitution and permutation are the main two operations applied, both or separately, on plain-texts in order to ensure confusion and diffusion.

While the terminology (substitution and permutation) used nowadays is roughly the same since centuries and the objective is to make the cipher-text the most complex and inintelligible, the confusion and diffusion terms are relatively recents. Of course, the approaches and techniques have seen a huge developpement during the long history of cryptology to ensure confusion and diffusion. As an example, the security of Advanced Encryption Standard (AES) [18], the most known and recent cryptographic standard, is mainly based on the robustness of S-boxes, the "Substitution" boxes. Diffusion in the AES SP-network is achieved by a linear transformation [44].

On another hand, some crytpographic systems use other approaches and techniques to guarantee a high degree of confusion and diffusion. In our system, we are in this category of cryptographic sytems. There is no permutation or substitution in the known sense of the terms, rather there is a new approach based on subspace concept to guarantee the same security objectives targeted by substitution and permutation i.e. confusion and diffusion.

In our proposed subspace-based encryption system, confusion is achieved by the linearity and and nonlinearity that obscure the relationship between the plain-text, the cipher-text and the key. Furthermore, we see from equation (5.1) that each value of the cipher-text $\mathbf{x}(t)$ depends on each value of the plain-text and the key what ensures the diffusion requirement.

In the following sections, the robustness, from a security point of view, of the proposed subspace-based cryptographic system is analysed and evaluated. Several tests using some cryptanalysis attacks are conducted on both orthogonal and oblique subspace-based encryption systems, for both iterative and simple versions.

5.2 Cipher-text-only attack

This is the most known and realistic attack since it does not require more than the availability of cipher-texts which can be obtained by a system similar to the system which is under attack or even by interception of cipher-texts. Generally, communications are using public infrastructures and protocols (e.g. telephone networks, internet) and hence, could be intercepted.

5.2.1 Sensitivity to $\mathbf{P}_{A(t)}$

If two distinct keys are used to encrypt the same plain-text, the sensitivity of a cryptosystem to its secret key is evaluated in accordance to the difference between the two encrypted signals obtained from encrypting the same plain-text. This means that given two distinct keys, even if their difference is the minimal value under the current finite precision, the encryption and decryption results of a robust cryptosystem should still be completely different [11, 17].

In other words, a robust cryptosystem, from a cryptographic point of view, should have a high sensitivity to the secret key [11, 17]. A very low sensitivity means that a mismatched key can approximately recover the plain-text. In the sequel, we show that the involved computation in our proposed subspace-based encryption scheme is very sensitive to projection mismatch.

Orthogonal subspace-based encryption scheme

Let us first rewrite for ease of use the encryption equation (3.2) as:

$$\mathbf{x}(t) = \mathbf{y}_p(t) + \beta \mathbf{z}(t) \tag{5.1}$$

where $\mathbf{y}_p(t) = \mathbf{A}(t)\mathbf{p}(t)$ and $\mathbf{z}(t) = \mathbf{P}^{\perp}_{A(t)}\mathbf{B}(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{p}(t))]$. Consider the following mismatched projector

$$\hat{\mathbf{P}}_{A(t)} = \mathbf{P}_{A(t)} + \epsilon \mathbf{I} \tag{5.2}$$

with ϵ a finite precision value and $\mathbf{I}$ a $(M+1) \times (M+1)$ identity matrix. Using the mismatched projector $\hat{\mathbf{P}}_{A(t)}$ for decryption, one gets:

$$\begin{aligned} \hat{\mathbf{P}}_{A(t)}\mathbf{x}(t) &= (\mathbf{P}_{A(t)} + \epsilon \mathbf{I})\mathbf{y}_p(t) + \beta(\mathbf{P}_{A(t)} + \epsilon \mathbf{I})\mathbf{z}(t) \\ &= (1+\epsilon)\mathbf{y}_p(t) + \beta\epsilon \mathbf{z}(t) \end{aligned} \tag{5.3}$$

In equation (5.3), we have used the fact that $\mathbf{P}_{A(t)}\mathbf{y}_p(t) = \mathbf{y}_p(t)$ and $\mathbf{P}_{A(t)}\mathbf{z}(t) = 0$. Note from the same equation (5.3) that the decrypted data by the mismatched projector is still encrypted according to the proposed encryption equation (3.2).

By choosing $\beta = O(\frac{1}{\epsilon})$, equation (5.3) shows that, even for a very small value of ϵ, there is a very significant difference between the decryption results obtained by the actual projector $\mathbf{P}_{A(t)}$ and its mismatched version $\hat{\mathbf{P}}_{A(t)}$. This means that the proposed subspace-based encryption scheme is very sensitive to projector mismatch. Hence, it verifies an important principle of cryptographic robustness that is the high sensitivity to secret parameter mismatch. This high sensitivity is checked by using the following experiment procedure [11]:

Step 1: For a randomly-generated projector and keys $(\mathbf{P}_{A(t)}, \mathbf{k}(t))$, compute the cipher-text $\mathbf{x}(t)$ corresponding to a plain-text $\mathbf{p}(t)$.

Step 2: With a mismatched projector $\mathbf{P}_{A(t)} + \epsilon\mathbf{I}$, decrypt $\mathbf{x}(t)$ to get $\hat{\mathbf{p}}(t)$, an estimated version of $\mathbf{p}(t)$, where $\epsilon \in [0, 1]$.

Detailed results and discussion of this experiment are shown in chapter 6.

Iterative orthogonal subspace-based encryption scheme

For the iterative orthogonal subspace-based encryption scheme, let us rewrite the encryption equation:

$$\mathbf{x}_n(t) = \mathbf{A}_n(t)\mathbf{x}_{(n-1)}(t) + \beta\mathbf{P}^{\perp}_{A_n(t)}\mathbf{B}_n(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{x}_{(n-1)}(t))]$$

where $\mathbf{x}_n(t)$ and $\mathbf{x}_{(n-1)}(t)$ denote the n^{th} and $(n-1)^{th}$ encrypted segments. $n \geq 1$ and $\mathbf{x}(0)= \mathbf{p}(t)$, the plain-text. as:

$$\mathbf{x}_n(t) = \mathbf{y}_{(p,n)}(t) + \beta\mathbf{z}_n(t) \tag{5.4}$$

where $\mathbf{y}_{(p,n)}(t) = \mathbf{A}_n(t)\mathbf{x}_{(n-1)}(t)$
and
$\mathbf{z}_n(t) = \mathbf{P}^{\perp}_{A_n(t)}\mathbf{B}_n(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{x}_{(n-1)}(t))]$.
If we consider the following mismatched projector

$$\hat{\mathbf{P}}_{\mathbf{A}_n(t)} = \mathbf{P}_{\mathbf{A}_n(t)} + \epsilon\mathbf{I} \tag{5.5}$$

with ϵ a finite precision value and $\mathbf{I}$ a $(M+1)\times(M+1)$ identity matrix. The decrypted data $\mathbf{x}_{(p,n)}$ using the mismatched projector is then given by $\hat{\mathbf{P}}_{\mathbf{A}_n(t)}\mathbf{x}_n(t)$. one gets:

$$\begin{aligned}\hat{\mathbf{P}}_{\mathbf{A}_n(t)}\mathbf{x}_n(t) &= (\mathbf{P}_{\mathbf{A}_n(t)}+\epsilon\mathbf{I})\mathbf{y}_{(p,n)}(t)+\beta(\mathbf{P}_{\mathbf{A}_n(t)}+\epsilon\mathbf{I})\mathbf{z}_n(t)\\ &= (1+\epsilon)\mathbf{y}_{(p,n)}(t)+\beta\epsilon\mathbf{z}_n(t)\end{aligned} \tag{5.6}$$

Note from equation (5.6) that the decrypted data by the mismatched projector is still encrypted according to the proposed encryption equation (3.2).

By choosing $\beta = O(\frac{1}{\epsilon})$, equation (5.6) shows that, even for a very small value of ϵ, there is a very significant difference between the decryption results obtained by the actual projector $\mathbf{P}_{\mathbf{A}_n(t)}$ and its mismatched version $\hat{\mathbf{P}}_{\mathbf{A}_n(t)}$. Note that the iteration on n makes an accumulation on the initial mismatch on the projector and hence makes the encryption more sensitive to projector mismatch.

Adopting the same methodology applied for the orthogonal subspace-based encryption scheme to check the high sensitivity of iterative orthogonal subspace-based encryption scheme to key mismatch, the following procedure is applied:

Step 1: Generate random projector and keys $(\mathbf{P}_{\mathbf{A}_n(t)}, \mathbf{k}(t))$, then compute the cipher-text $\mathbf{x}_n(t)$ corresponding to a plain-text $\mathbf{p}(t)$.

Step 2: Using a mismatched projector $\mathbf{P}_{\mathbf{A}_n(t)}+\epsilon\mathbf{I}$, decrypt $\mathbf{x}_n(t)$ to get $\hat{\mathbf{p}}(t)$, an estimated version of $\mathbf{p}(t)$, where $\epsilon\in[0,1]$.

Detailed results and discussion of this experiment are shown in chapter 6.

Oblique subspace-based encryption scheme

Let us rewrite the encryption equation (4.5) as:

$$\mathbf{x}(t) = \mathbf{y}_p(t)+\beta\mathbf{z}(t) \tag{5.7}$$

where $\mathbf{y}_p(t) = \mathbf{A}(t)\mathbf{p}(t)$ and $\mathbf{z}(t) = \mathbf{B}(t)[\mathbf{k}(t)\odot\mathbf{g}(\mathbf{p}(t))]$. $\mathbf{A}(t)$ and $\mathbf{B}(t)$ are $(M+1)\times M$ and $(M+1)\times 1$ full rank key matrices, respectively. Following the same methodology as in the orthogonal approach, let us consider the mismatched oblique projector:

$$\hat{\mathbf{E}}_{A(t)B(t)} = \mathbf{E}_{A(t)B(t)}+\epsilon\mathbf{I} \tag{5.8}$$

with ϵ a finite precision value and $\mathbf{I}$ a $(M+1) \times (M+1)$ identity matrix. The mismatched projector $\hat{\mathbf{E}}_{A(t)B(t)}$ is used for decryption; one gets:

$$\begin{aligned} \hat{\mathbf{E}}_{A(t)B(t)}\mathbf{x}(t) &= (\mathbf{E}_{A(t)B(t)} + \epsilon\mathbf{I})\mathbf{y}_p(t) \\ &+ \beta(\mathbf{E}_{A(t)B(t)} + \epsilon\mathbf{I})\mathbf{z}(t) \\ &= (1+\epsilon)\mathbf{y}_p(t) + \beta\epsilon\mathbf{z}(t) \end{aligned} \tag{5.9}$$

In equation (5.9) , we have used the fact that $\mathbf{E}_{A(t)B(t)}\mathbf{y}_p(t) = \mathbf{y}_p(t)$ and $\mathbf{E}_{A(t)B(t)}\mathbf{z}(t) = 0$. Note from the same equation (5.9) that the decrypted data obtained from the use of a very small-mismatched oblique projector is still encrypted according to the oblique subspace-based encryption equation (4.5).

For a very small value of ϵ, by choosing $\beta = O(\frac{1}{\epsilon})$, equation (5.9) shows that there is a very significant difference between the decryption results obtained by the actual oblique projector $\mathbf{E}_{A(t)B(t)}$ and its mismatched version $\hat{\mathbf{E}}_{A(t)B(t)}$. This leads to say that this oblique subspace-based encryption scheme is very sensitive to projector mismatch i.e. this encryption scheme fulfils the requirement of high sensitivity to secret parameter mismatch.

Adopting the same methodology of experimentation used previously for orthogonal subspace-based encryption scheme to check the high sensitivity of oblique subspace-based encryption scheme to projector mismatch, the following procedure is applied:

Step 1: Generate random projector and keys $(\mathbf{E}_{A(t)B(t)}, \mathbf{k}(t))$, and compute the cipher-text $\mathbf{x}(t)$ which corresponds to a plain-text $\mathbf{p}(t)$.

Step 2: Decrypt $\mathbf{x}(t)$ to get $\hat{\mathbf{p}}(t)$, an estimated version of $\mathbf{p}(t)$, by using the mismatched projector $\mathbf{E}_{A(t)B(t)} + \epsilon\mathbf{I}$, where $\epsilon \in [0, 1]$.

Results of this experimentation are shown and discussed in chapter 6.

Iterative oblique subspace-based encryption scheme

For the iterative oblique subspace-based encryption scheme, let us rewrite the encryption equation (4.9) as:

$$\mathbf{x}_n(t) = \mathbf{y}_n(t) + \beta\mathbf{z}_n(t) \tag{5.10}$$

where $\mathbf{y}_n(t) = \mathbf{A}_n(t)\mathbf{x}_{(n-1)}(t)$ and $\mathbf{z}_n(t) = \mathbf{B}_n(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{x}_{(n-1)}(t))]$. Let us consider a mismatched oblique projector:

$$\hat{\mathbf{E}}_{\mathbf{A}_n(t)\mathbf{B}_n(t)} = \mathbf{E}_{\mathbf{A}_n(t)\mathbf{B}_n(t)} + \epsilon\mathbf{I} \tag{5.11}$$

with ϵ a finite precision value and $\mathbf{I}$ a $(M+1)\times(M+1)$ identity matrix. The decrypted data $\mathbf{x}_{(p,n)}(t)$ obtained from applying the mismatched projector is then given by $\hat{\mathbf{E}}_{\mathbf{A}_n(t)\mathbf{B}_n(t)}\ \mathbf{x}_n(t)$. One gets:

$$\begin{aligned}\hat{\mathbf{E}}_{\mathbf{A}_n(t)\mathbf{B}_n(t)}\mathbf{x}_n(t) &= (\mathbf{E}_{\mathbf{A}_n(t)\mathbf{B}_n(t)} + \epsilon\mathbf{I})\mathbf{y}_{(p,n)}(t) \\ &+ \beta(\mathbf{E}_{\mathbf{A}_n(t)\mathbf{B}_n(t)} + \epsilon\mathbf{I})\mathbf{z}_n(t) \\ &= (1+\epsilon)\mathbf{y}_{(p,n)}(t) + \beta\epsilon\mathbf{z}_n(t) \end{aligned} \tag{5.12}$$

From equation (5.12), one can see that the decrypted data by the oblique mismatched projector is still encrypted according to the proposed iterative oblique encryption equation (4.9).

By choosing $\beta = O(\frac{1}{\epsilon})$, equation (5.12) shows that, even for a very small value of ϵ, this iterative oblique subspace-based encryption scheme presents very significant difference in the corresponding cipher-texts. Note that as in the case of the iterative orthogonal subspace-based encryption, the iteration on n makes an accumulation on the initial mismatch on the projector and hence makes the encryption more sensitive to projector mismatch. The same procedure followed previously is applied to show the high sensitivity of iterative oblique subspace-based encryption scheme to projector mismatch.

Step 1: Choose a number of iterations n ($n \geq 2$).

Step 2: Generate random oblique projector and keys $(\mathbf{E}_{\mathbf{A}_n(t)\mathbf{B}_n(t)}, \mathbf{k}(t))$, then compute the cipher-text $\mathbf{x}_n(t)$ corresponding to a plain-text $\mathbf{p}(t)$.

Step 3: Apply the iterative oblique decryption formula on $\mathbf{x}_n(t)$ to get $\hat{\mathbf{p}}(t)$, an estimated version of $\mathbf{p}(t)$, using the mismatched projector $\mathbf{E}_{\mathbf{A}_n(t)\mathbf{B}_n(t)} + \epsilon\mathbf{I}$ where $\epsilon \in [0, 1]$.

Results of this experimentation are shown and discussed in chapter 6.

5.2.2 Sensitivity to $\mathbf{k}(t)$

The subspace-based encryption scheme is also very sensitive to the key signals. This is due to the same reason of its high sensitivity to projector

$\mathbf{P}_{A(t)}$. Furthermore, The key signals $\mathbf{k}(t)$ are generated randomly for each plain-text through the random or the pseudo-random generator as shown in Figure (3.1). Let us re-write the encryption equation (3.2) for an orthogonal subspace-based encryption scheme:

$$\mathbf{x}(t) = \mathbf{A}(t)\mathbf{p}(t) + \beta\mathbf{P}^{\perp}_{A(t)}\mathbf{B}(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{p}(t))] \tag{5.13}$$

where $\mathbf{A}(t)$and $\mathbf{B}(t)$ are $(M+1)\times M$ and $(M+1)\times M$ full rank key matrices, respectively. $\mathbf{k}(t)$ is generated for each vector $\mathbf{x}(t)$. Consider now a second operation of encrypting the same plain-text $\mathbf{p}(t)$ using the same key matrix $\mathbf{A}(t)$. An expected result of this encryption operation should be the same cipher-text $\mathbf{x}(t)$ obtained as an output of the equation (5.13). However, this is not the case in our proposed subspace-based encryption scheme. The obtained cipher-text is given by the following equation:

$$\mathbf{x}_1(t) = \mathbf{A}(t)\mathbf{p}(t) + \beta\mathbf{P}^{\perp}_{A(t)}\mathbf{B}(t)[\mathbf{k}_1(t) \odot \mathbf{g}(\mathbf{p}(t))] \tag{5.14}$$

where the cipher-text $\mathbf{x}_1(t)$ is different from $\mathbf{x}(t)$ because the key signal $\mathbf{k}_1(t)$ is totally different from the key signal $\mathbf{k}(t)$ used in the first encryption. This is due to the random (or pseudo-random) generator used to generate the key signals that generates each time a different sequence of keys. More generally, the cipher-texts obtained from the use of the same plain-text and the same key matrix in a subspace-based encryption scheme are always different. This is an imporatnt feature which has an impact on the resistance of the proposed subspace encryption scheme to cipher-text only attack. Actually, a cryptanalyst gathering a set of let us say N cipher-texts has no information about the number of the corresponding plain-texts. This number could be the same number of cipher-texts or less. This uncertainty about the number of the corresponding plain-texts provides an additive level of resistance to this class of cryptanalysis attack.

5.2.3 Sensitivity to plain-text

Another cryptographic property required by a robust cryptosystem is that the encryption must be very sensitive to plain-text, i.e., the cipher-texts of two plain-texts with a slight difference should be much different [11, 17]. This property matches well with the proposed subspace-based encryption scheme.

Using the same key and given two plain-texts $p^{(1)}(t)$ and $p^{(2)}(t)$ with a very slight difference, the obtained result presents a significant sensitivity to this slight difference. It has been tested that no one could detect the slight difference between the two plain-texts (e.g. two speech signals). In other words, for a person, in the speech application, the two speech signals are actually the same. However, their encrypted versions are too different.

5.2.4 Differential attack

The difficulty of solving nonlinear equations can be useful for designing cryptosystems. A differential attack, is based on the assumption that two identical key signals are used to encrypt at least two plain-texts [11]. However, the key space of a good pseudo random number generator, which generates pseudo random sequences having statistical properties similar to those of random sequences, should be large enough to prevent the occurrence of two identical key signals. Moreover, even when we assume that two identical key signals have been used to encrypt two plain-texts, the differential attack can not be realized.

Orthogonal subspace-based encryption scheme

Let us assume that two plain-texts $\mathbf{p}^{(1)}(t)$ and $\mathbf{p}^{(2)}(t)$ are encrypted using the same key parameters $(\mathbf{P}_{A(t)}, \mathbf{k}(t))$. From equation (3.2), one has:

$$\mathbf{x}^{(1)}(t) = \mathbf{A}(t)\mathbf{p}^{(1)}(t) + \beta\mathbf{P}^{\perp}_{A(t)}\mathbf{B}(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{p}^{(1)}(t))] \tag{5.15}$$

and

$$\mathbf{x}^{(2)}(t) = \mathbf{A}(t)\mathbf{p}^{(2)}(t) + \beta\mathbf{P}^{\perp}_{A(t)}\mathbf{B}(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{p}^{(2)}(t))] \tag{5.16}$$

Combining equations (5.15) and (5.16), leads to

$$\Delta_{\mathbf{x}}(t) = \mathbf{A}(t)\Delta_{\mathbf{p}}(t) + \beta\mathbf{P}^{\perp}_{A(t)}\mathbf{B}(t)[\mathbf{k}(t) \odot [\mathbf{g}(\mathbf{p}^{(1)}(t)) - \mathbf{g}(\mathbf{p}^{(2)}(t))]] \tag{5.17}$$

where $\Delta_{\mathbf{x}}(t)$ is the cipher-text differential described as:

$$\Delta_{\mathbf{x}}(t) = \mathbf{x}^{(1)}(t) - \mathbf{x}^{(2)}(t) \tag{5.18}$$

and $\Delta_{\mathbf{p}}(t)$ is the plain-text differential described as:

$$\Delta_{\mathbf{p}}(t) = \mathbf{p}^{(1)}(t) - \mathbf{p}^{(2)}(t) \tag{5.19}$$

Note that even if the same key is used to obtain the cipher-texts $\mathbf{x}^{(1)}(t)$ and $\mathbf{x}^{(2)}(t)$, the additive subspace perturbation term is still present in equation (5.17). Moreover, the plain-text differential $\Delta_{\mathbf{p}}(t)$ can not be computed because of the permanent presence of the terms $\mathbf{p}^{(1)}(t)$ and $\mathbf{p}^{(2)}(t)$ in equation (5.17). This is due, as mentioned in section (3.1), to the existing correlation between the additive subspace perturbation term and the plain-text term of the proposed encryption equation (3.2).

Iterative orthogonal subspace-based encryption scheme

By assuming that two plain-texts $\mathbf{p}^{(1)}(t)$ and $\mathbf{p}^{(2)}(t)$ are encrypted using the same key parameters $(\mathbf{P}_{\mathbf{A}_n(t)}, \mathbf{k}(t))$. From equation (3.9), one has:

$$\mathbf{x}_n^{(1)}(t) = \mathbf{A}_n(t)\mathbf{x}_{(n-1)}^{(1)}(t) + \beta\mathbf{P}_{\mathbf{A}_n(t)}^{\perp}\mathbf{B}_n(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{x}_{(n-1)}^{(1)}(t))] \tag{5.20}$$

where $\mathbf{x}_n^{(1)}(t)$ and $\mathbf{x}_{(n-1)}^{(1)}$ denote the n^{th} and $(n-1)^{th}$ encrypted segments of the first plain-text. $n \geq 1$ and $\mathbf{x}^{(1)}(0)= \mathbf{p}^{(1)}(t)$ is the first plain-text.

And

$$\mathbf{x}_n^{(2)}(t) = \mathbf{A}_n(t)\mathbf{x}_{(n-1)}^{(2)}(t) + \beta\mathbf{P}_{\mathbf{A}_n(t)}^{\perp}\mathbf{B}_n(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{x}_{(n-1)}^{(2)}(t))] \tag{5.21}$$

where $\mathbf{x}_n^{(2)}(t)$ and $\mathbf{x}_{(n-1)}^{(2)}$ denote the n^{th} and $(n-1)^{th}$ encrypted segments of the second plain-text. $n \geq 1$ and $\mathbf{x}^{(2)}(0)= \mathbf{p}^{(2)}(t)$, the second plain-text.

Combining equations (5.20) and (5.21), one gets

$$\begin{aligned} \Delta_{\mathbf{x}_n}(t) &= \mathbf{A}_n(t)\Delta_{\mathbf{x}_{(n-1)}}(t) \\ &+ \beta\mathbf{P}_{\mathbf{A}_n(t)}^{\perp}\mathbf{B}_n(t)[\mathbf{k}(t) \odot [\mathbf{g}(\mathbf{x}_{(n-1)}^{(1)}(t)) - \mathbf{g}(\mathbf{x}_{(n-1)}^{(2)}(t))]] \end{aligned} \tag{5.22}$$

where $\Delta_{\mathbf{x}_n(t)}$ and $\Delta_{\mathbf{x}_{(n-1)}}$ are the cipher-text differentials described as:

$$\Delta_{\mathbf{x}_n(t)} = \mathbf{x}_n^{(1)}(t) - \mathbf{x}_n^{(2)}(t) \tag{5.23}$$

and

$$\Delta_{\mathbf{x}_{(n-1)}}(t) = \mathbf{x}_{(n-1)}^{(1)}(t) - \mathbf{x}_{(n-1)}^{(2)}(t) \tag{5.24}$$

where

$$\begin{aligned}\Delta_{\mathbf{x}_0(t)} &= \mathbf{x}_0^{(1)}(t) - \mathbf{x}_0^{(2)}(t) \\ &= \mathbf{p}^{(1)}(t) - \mathbf{p}^{(2)}(t) \\ &= \Delta_{\mathbf{p}}(t) \end{aligned} \tag{5.25}$$

One can see that even if the same key is used to obtain the cipher-texts $\mathbf{x}_n^{(1)}(t)$ and $\mathbf{x}_n^{(2)}(t)$, the additive subspace perturbation term is still present in equation (5.22). Moreover, the plain-text differential $\Delta_{\mathbf{p}}(t)$ can not be computed because of the permanent presence of the terms $\mathbf{p}^{(1)}(t)$ and $\mathbf{p}^{(2)}(t)$ in equation (5.22). This is due, as mentioned in section (3.2), to the existing correlation between the additive subspace perturbation term and the plain-text term of the proposed encryption equation (3.9).

Oblique subspace-based encryption scheme

Let us assume that two plain-texts $\mathbf{p}^{(1)}(t)$ and $\mathbf{p}^{(2)}(t)$ are encrypted using the same key parameters $(\mathbf{E}_{\mathbf{A}(t)\mathbf{B}(t)}, \mathbf{k}(t))$. From equation (4.5), one has:

$$\mathbf{x}^{(1)}(t) = \mathbf{A}(t)\mathbf{p}^{(1)}(t) + \beta\mathbf{B}(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{p}^{(1)}(t))] \tag{5.26}$$

and

$$\mathbf{x}^{(2)}(t) = \mathbf{A}(t)\mathbf{p}^{(2)}(t) + \beta\mathbf{B}(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{p}^{(2)}(t))] \tag{5.27}$$

Combining equations (5.26) and (5.27), gives

$$\Delta_{\mathbf{x}}(t) = \mathbf{A}(t)\Delta_{\mathbf{p}}(t) + \beta\mathbf{B}(t)[\mathbf{k}(t) \odot [\mathbf{g}(\mathbf{p}^{(1)}(t)) - \mathbf{g}(\mathbf{p}^{(2)}(t))]] \tag{5.28}$$

where $\Delta_{\mathbf{x}}(t)$ is the cipher-text differential described as:

$$\Delta_{\mathbf{x}}(t) = \mathbf{x}^{(1)}(t) - \mathbf{x}^{(2)}(t) \tag{5.29}$$

and $\Delta_{\mathbf{p}}(t)$ is the plain-text differential described as:

$$\Delta_{\mathbf{p}}(t) = \mathbf{p}^{(1)}(t) - \mathbf{p}^{(2)}(t) \tag{5.30}$$

Note that the additive oblique subspace perturbation term is still present in equation (5.28) even if the same key is used to obtain the cipher-texts $\mathbf{x}^{(1)}(t)$ and $\mathbf{x}^{(2)}(t)$. Moreover, the first term $\Delta_{\mathbf{p}}(t)$ could not be computed because of the permanent presence of $\mathbf{p}^{(1)}(t)$ and $\mathbf{p}^{(2)}(t)$ in equation (5.28). The existing correlation between the additive oblique subspace term and the plain-text term in this encryption scheme presents a protection against differential attack.

Iterative oblique subspace-based encryption scheme

Assuming that two plain-texts $\mathbf{p}^{(1)}(t)$ and $\mathbf{p}^{(2)}(t)$ are encrypted using the same key parameters $(\mathbf{E}_{A_n(t)B_n(t)}, \mathbf{k}(t))$, from equation (4.9), one gets:

$$\mathbf{x}_n^{(1)}(t) = \mathbf{A}_n(t)\mathbf{x}_{(n-1)}^{(1)}(t) + \beta\mathbf{B}_n(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{x}(n-1)^{(1)}(t))] \tag{5.31}$$

and

$$\mathbf{x}_n^{(2)}(t) = \mathbf{A}_n(t)\mathbf{x}_{(n-1)}^{(2)}(t) + \beta\mathbf{B}_n(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{x}(n-1)^{(2)}(t))] \tag{5.32}$$

Combining equations (5.31) and (5.32), gives

$$\begin{aligned} \Delta_{\mathbf{x}_n}(t) &= \mathbf{A}_n(t)\Delta_{\mathbf{x}_{(n-1)}}(t) \\ &+ \beta\mathbf{B}_n(t)[\mathbf{k}(t) \odot [\mathbf{g}(\mathbf{x}_{(n-1)}^{(1)}(t)) - \mathbf{g}(\mathbf{x}_{(n-1)}^{(2)}(t))] \end{aligned} \tag{5.33}$$

where $\Delta_{\mathbf{x}_n(t)}$ is the cipher-text differential described as:

$$\Delta_{\mathbf{x}_n(t)} = \mathbf{x}_n^{(1)}(t) - \mathbf{x}_n^{(2)}(t) \tag{5.34}$$

and $\Delta_{\mathbf{x}_{(n-1)}} = \mathbf{x}_{(n-1)}^{(1)}(t) - \mathbf{x}_{(n-1)}^{(2)}(t)$ for $n \geq 1$.

For $n = 1$, the following equation

$$\Delta_{\mathbf{x}_0}(t) = \mathbf{x}_0^{(1)}(t) - \mathbf{x}_0^{(2)}(t) = \mathbf{p}^{(1)}(t) - \mathbf{p}^{(2)}(t)$$

describes the plain-text differential. This becomes the same case as in the oblique subspace-based encryption scheme.

For $n \geq 1$, the cipher-text differential could not be computed because of the presence of the additive oblique subspace perturbation term even the same key is used in the encryption process. This protection against differential attack is guaranteed by the existing correlation between the additive perturbation term and the plain-text term.

Added-value of non linear function $\mathbf{g}(.)$

During the conception process of this subspace-based encryption scheme, the choice of the nonlinearity has been an important step. On one side, it has to

ensure a high degree of nonlinearity and on the other side it has to prevent, or at least to make very difficult, the use of known cryptanalysis attacks. A condition which we have stated to select the nonlinear function $\mathbf{g}(\mathbf{p}(t))$ is that it verifies $\mathbf{g}(0) = 0$.

Actually, one can choose any non-linearity that verifies the above condition and ensures a correlation between the two terms of equation (3.2). The choice of an indicator function for example does not fulfill these requirements because it will make the additive second term of equation (3.2) uncorrelated with the first term. One of our objectives is to make these two terms correlated in order to prevent their recovery from, to our knowledge, any statistical signal processing techniques. Also, this correlation between the two terms makes the proposed system robust to differential attack as shown in subsection (5.2.4).

The importance of the condition described above for selecting the nonlinear function $\mathbf{g}(\mathbf{p}(t))$ i.e. $\mathbf{g}(0) = 0$ could be explained via an inverse example. For example, assuming that $\mathbf{g}(0) \neq 0$ and the second term of equation (3.2) lives in a M-L dimensional subspace and there is no contents presented to encryption, then equation (3.2) reads:

$$\mathbf{x}(t) = \beta \mathbf{P}^{\perp}_{A(t)} \mathbf{B}(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{p}(t))]$$

Hence, a Principal Component Analysis will provide a projector on the subspace spanned by $\mathbf{P}^{\perp}_{A}\mathbf{B}$ that is orthogonal to the space spanned by matrix $\mathbf{A}$. Since only a projector on the space spanned by $\mathbf{A}$ that is needed for the decryption, this will crack the algorithm. To overcome this problem, the condition $\mathbf{g}(p_i(t)) = 0$ if $p_i(t) = 0$ has been set. Hence, if no plain-text is presented in the encryption equation (3.2) (i.e. $\mathbf{p}(t) = 0$), the cryptosystem will provide no contents (i.e. $\mathbf{x}(t) = 0$).

To our knowledge, the aforementioned problem has no solution yet from a statistical signal processing point of view. This important property allows to ban the use of any signal processing-based cryptanalysis technique in absence of plain-text.

Chapter 6

Application and Performance Evaluation

This chapter presents the results of the experimentations conducted on the proposed subspace-based encryption method for the four proposed schemes: orthogonal, iterative orthogonal, oblique and iterative oblique subspace-based encryption schemes. These experimentations target to assess the proposed schemes by evaluating aspects related to both security robustness from a cryptographic point of view and quality of reconstruction of plain-texts at the decryption level.

For security assessment purpose, the evaluation approach adopts some cryptanalysis attacks. For quality assessment, the evaluation process uses both subjective and objective measurements. The tests and experimentations were conducted on speech signals, images and binary phase shift keying data.

6.1 Application to speech signal

Security robustness evaluation

In practice, ϵ the finite precision value that would be used in the cryptanalysis by exhaustive search, varies usually from 0.1 to 0.01. If ϵ is chosen too small, the key space becomes huge and the cryptanalysis by exhaustive search becomes impracticable.

Table 6.1: SNR(dB) of four original speech segments in four encrypted segments and four decrypted segments.

	$x_1(t)$	$x_2(t)$	$x_3(t)$	$x_4(t)$	$x_p(t)$
$p_1(t)$	-204.28	-189.76	-183.23	-206.62	404.25
$p_2(t)$	-208.66	-193.14	-186.61	-210.00	361.62
$p_3(t)$	-216.20	-200.68	-194.14	-217.54	341.09
$p_4(t)$	-207.39	-191.87	-185.34	-208.73	352.03

The decryption requires a matrix pseudo-inversion. This might be expensive (especially if M is large) and might result in numerical problems if A(t) is ill-conditioned. However, the numerical problems that could rise from the possible ill-conditioning of matrix A(t) depend on the quality of the random or pseudo-random generator. In our experiments, M is chosen equal to 4, we have also run experiments with $M = 2$ and there were no significant effects on the encryption performance.

Quality performance analysis

In the objective evaluation, signal-to-noise ratio (dB) was used. The signal-to-noise ratio (SNR) in dB of each original segment in both the decrypted segments and encrypted ones is computed. Results of this computation is shown in Table 6.1.

The results are obtained from the use of the subspace-based encryption when applied on a speech file containing a record of a person saying lyrics of a child song in english (the child song is entitled "let's laugh together").

The original signal was sampled at a rate of 22.05 KHz and the number of bits per sample used to encode the data in the file was 16 bits/sample. One can see that the original segments are well covered using the proposed subspace-based method. In the decrypted segments, one can see that the signals are recovered with a very high SNR which ensures excellent voice quality in the case of speech encryption. On the other hand, the encrypted segments present a very low SNR.

For the subjective evaluation, a listening test through the subjective Degradation Category Rating (DCR) was conducted by using a 5-point scale for

evaluating the degradation: degradation is inaudible (5), degradation is audible but not annoying (4), degradation is slightly annoying (3), degradation is annoying (2), and degradation is very annoying (1) [7, 45]. The Degradation Mean Opinion Score (DMOS) represents the mean value of the results obtained from the listener's appreciation.

For this purpose, twenty listeners, ten male and ten female, were invited to give their scoring after hearing the original speech and the decrypted one. The DMOS obtained from this testing was 5. Thus, the excellent voice quality was also approved by the listeners.

Figure (6.1) shows results obtained from applying orthogonal subspace encryption on the speech file described in section (6.1) with a factor β equal to 10^6. Figure (6.1)-(a) shows the original signal whereas Figure (6.1)-(b) shows the key signals $\mathbf{k}(t)$ used during encryption. Figure (6.1)-(c) shows the signal encrypted according to equation (3.2) with a segment length $M = 4$. Note also that the encrypted signal has more samples than the original one, actually L samples more where L is the segment number. This sample excess comes from the fact that the dimension of the key matrices $\mathbf{A}(t)$ is $(M + 1) \times M$. After decryption with the proposed subspace method, the recovered signal is shown in Figure (6.1)-(d). As one can see from this figure, there is no visual difference between the original speech and the decrypted one.

Figure (6.2) shows results obtained from applying iterative orthogonal subspace encryption on the same speech file used in orthogonal subspace encryption with a factor β equal to 10^6. Figure (6.2)-(a) shows the original signal whereas Figures (6.2)-(b) and (c) show the key signals $\mathbf{k}(t)$ used during encryption and the obtained encrypted signal, respectively according to equation (3.9) with a segment length $M = 4$ and 2 rounds encryption. Note that, as mentioned in the orthogonal subspace encryption, the encrypted signal has also more samples than the original one. Figure (6.2)-(d) shows the recovered signal after decryption. One can see similarity between the original speech and the decrypted one.

Figure (6.3) shows results obtained from applying oblique subspace encryption on the speech file described in section (6.1) with a factor β equal to 10^6. Figure (6.3)-(a) shows the original signal whereas Figure (6.3)-(b) shows the

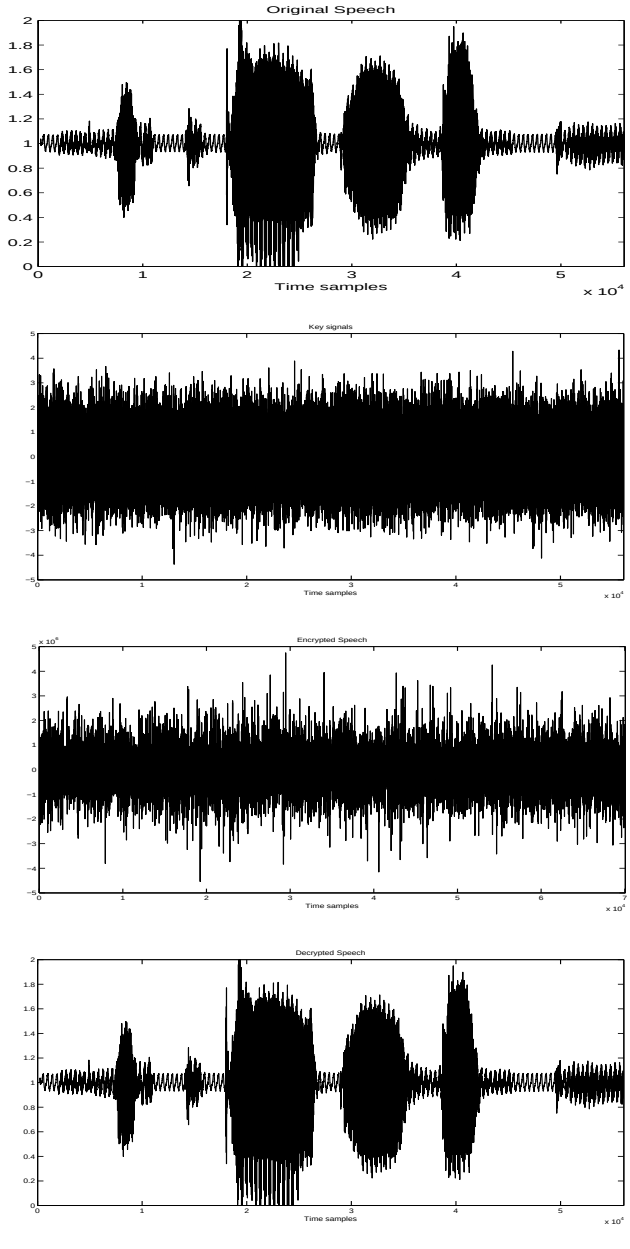


Figure 6.1: An example of orthogonal subspace-based speech encryption, (a) Original speech, (b) Key signals, (c) Encrypted speech, (d) Decrypted speech.

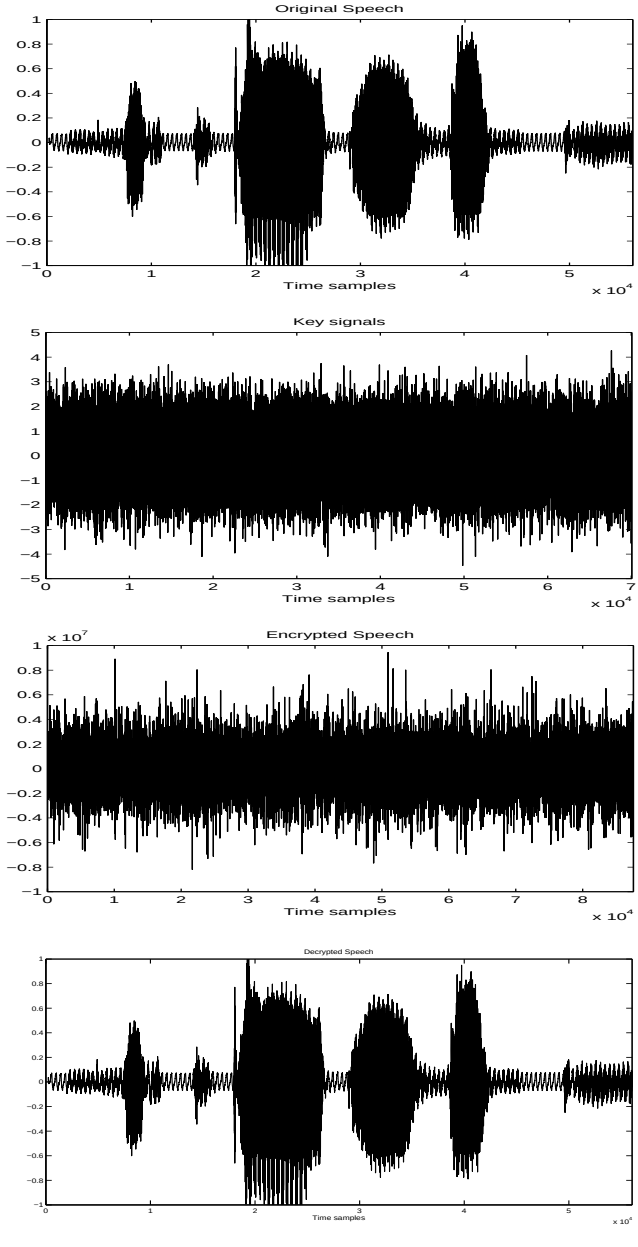


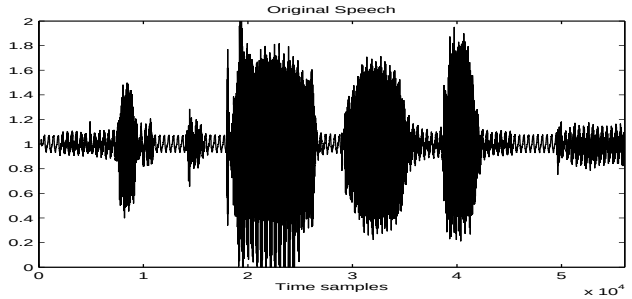
Figure 6.2: An example of iterative orthogonal subspace-based speech encryption with 2 iterations, (a) Original speech, (b) Key signals, (c) Encrypted speech, (d) Decrypted speech.

key signals $\mathbf{k}(t)$ used during encryption. Figure (6.3)-(c) shows the signal encrypted according to equation (4.5) with a segment length $M = 4$. Note that the encrypted signal has more samples than the original one, actually L samples more where L is the segment number. This sample excess comes, as mentioned for the orthogoanl subspace encryption, from the fact that the dimension of the key matrices $\mathbf{A}(t)$ is $(M + 1) \times M$. After decryption with the proposed oblique subspace method, the recovered signal is shown in Figure (6.3)-(d). As one can see from this figure, there is no visual difference between the original speech and the decrypted one.

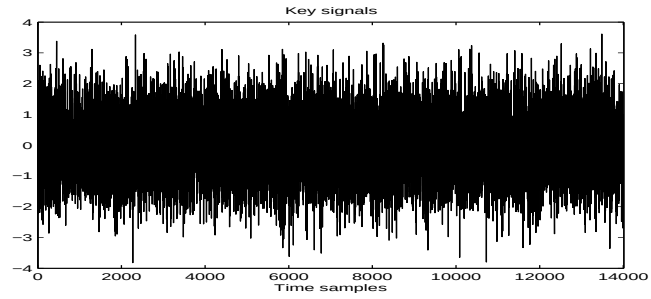
Figure (6.4) shows results obtained from applying iterative oblique subspace encryption on the same speech file used in oblique subspace encryption with a factor β equal to 10^6. Figure (6.4)-(a) shows the original signal whereas Figures (6.4)-(b) and (c) show the key signals $\mathbf{k}(t)$ used during encryption and the obtained encrypted signal, respectively according to equation (4.9) with a segment length $M = 4$ and 2 rounds encryption ($n = 2$). Note that, as mentioned in the orthogonal subspace encryption, the encrypted signal has also more samples than the original one. Figure (6.4)-(d) shows the recovered signal after decryption. Visually, there is no difference between the original speech and the decrypted one.

In order to assess the impact and to see the differences in using either orthogonal or oblique-based encryption, for 1-round or iterative approach, a two-steps comparison is made. This means that, first, a comparison is made within the same approach (orthogonal or oblique) between 1-round and iterative approaches. Second, a comparison is made between orthogonal and oblique-based encryptions, for both 1-round and iterative approaches.

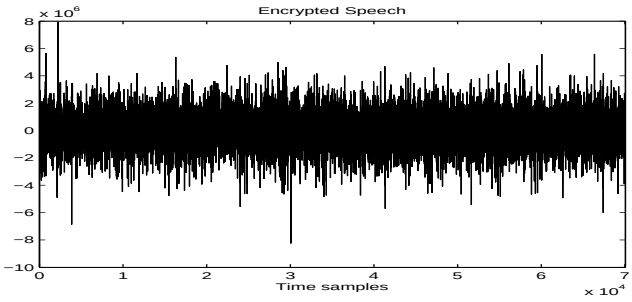
Following this methodology, as a comparison between the cipher-texts and their corresponding decrypted signals obtained from the use of orthogonal and iterative orthogonal subspace-based encryption for different iterations, Figure (6.5) shows the results for 1-round, 2-rounds, 3-rounds and 4-rounds encryption respectively. One can see that the amplitude level of the encrypted signal increases proportionally to the number of iterations. Actually, the amplitude level is multiplied by a factor 2 when the number of iterations increases by 1. At the decryption side, the original signal is recovered and no visual difference is found between the recovered signals of the different iterations.



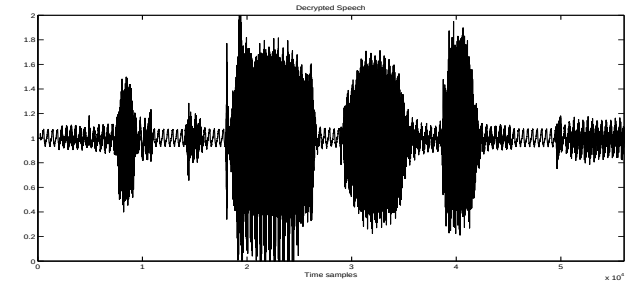
(a)



(b)



(c)



(d)

Figure 6.3: An example of oblique subspace-based speech encryption, (a) Original speech, (b) Key signals, (c) Encrypted speech, (d) Decrypted speech.

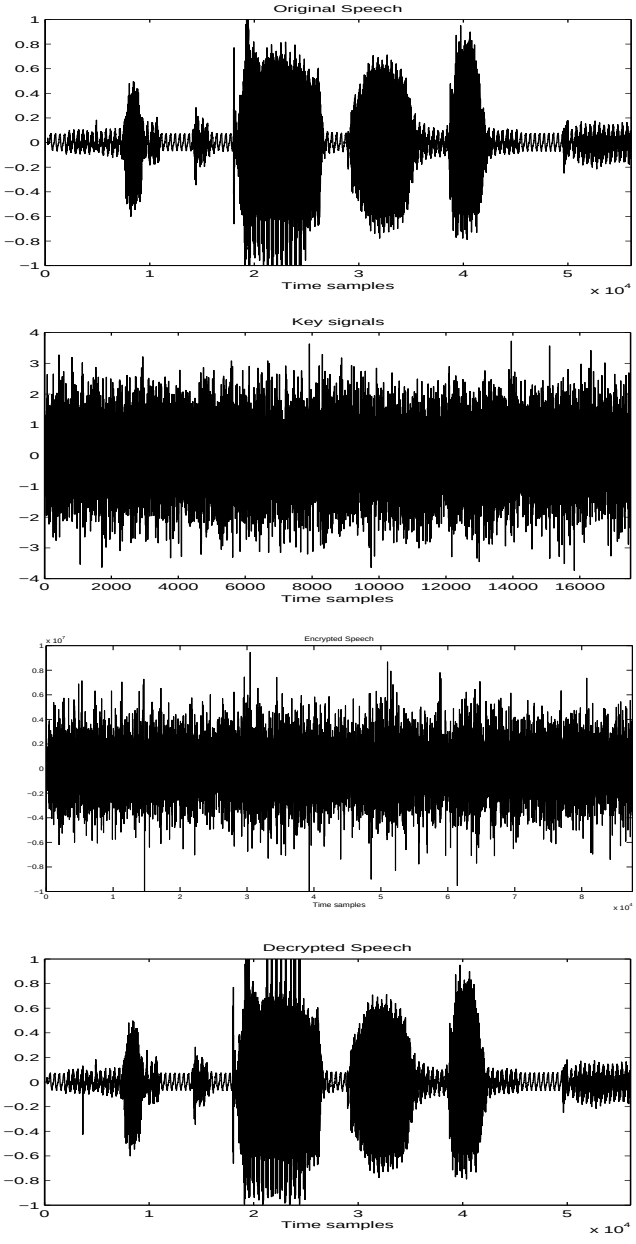


Figure 6.4: An example of iterative oblique subspace-based speech encryption with 2 iterations, (a) Original speech, (b) Key signals, (c) Encrypted speech, (d) Decrypted speech.

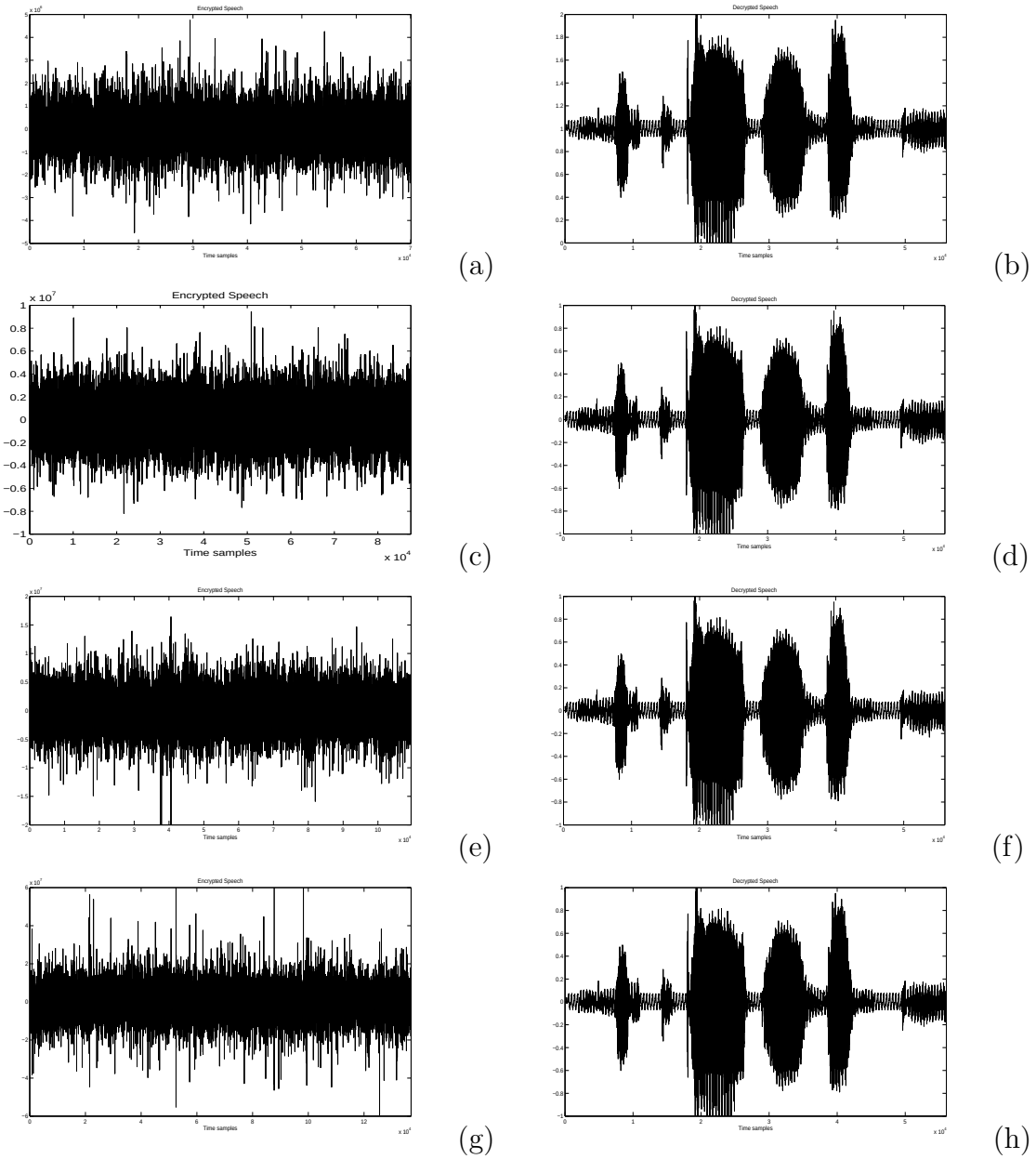


Figure 6.5: A comparison between cipher-texts and recovered signals for orthogonal and iterative orthogonal subspace-based speech encryption, (a)-(b) 1-round, (c)-(d) 2-rounds, (e)-(f) 3-rounds, (g)-(h) 4-rounds.

Figure (6.6) shows the ciphert-texts and their corresponding decrypted signals when we use the oblique and iterative oblique subspace-based encryption for different iterations: 1-round, 2-rounds, 3-rounds and 4-rounds encryption respectively. As it is mentioned in the orthogonal-based encryption scheme, one can see in Figure (6.6) that the amplitude level of the encrypted signal is proportional to the the number of iterations, actually by a factor 2. If the iterations number increases by 1, the amplitude level is multiplied by a factor 2. Whereas in the decryption side, one can see that there is no significant difference between the recovered signals of the different iterations.

Figure (6.7) shows a comparison between the ciphert-texts obtained from the use of iterative orthogonal and iterative oblique subspace-based encryption schemes for different iterations: 1-round, 2-rounds, 3-rounds and 4-rounds encryption respectively. One can see that the amplitude level of the oblique-based encryption scheme is higher than the amplitude level of the orthogonal-based encryption scheme when considering the same iterations number.

Whereas Figure (6.8) shows a comparison between the corresponding decrypted signals when we apply iterative orthogonal and iterative oblique subspace-based encryption schemes for different iterations: 1-round, 2-rounds, 3-rounds and 4-rounds encryption respectively. One can see that roughly, the decrypted signals are well recovered.

Figures (6.9) and (6.10) show a comparison in terms of sensitivity levels to plain-text mismatches of respectively 0.1 and 0.01 between iterative orthogonal subspace-based encryption schemes for different iterations: 1-round, 2-rounds, 3-rounds and 4-rounds encryption. One can see that, for the same level of plain-text mismatch, the sensitivity of the orthogonal-based encryption scheme, revealed by the cipher-text difference level, increases when the number of iterations rises. On the other side, even when the plain-text mismatch level decreases (from 0.1 to 0.01), the sensitivity decreases but remains at high levels, with a cipher-text difference varying roughly between 10^4 and 10^7.

Figure (6.11) and Figure (6.12) show a comparison in terms of sensitivity levels to plain-text mismatches of respectively 0.1 and 0.01 between iterative orthogonal and iterative oblique subspace-based encryption schemes for

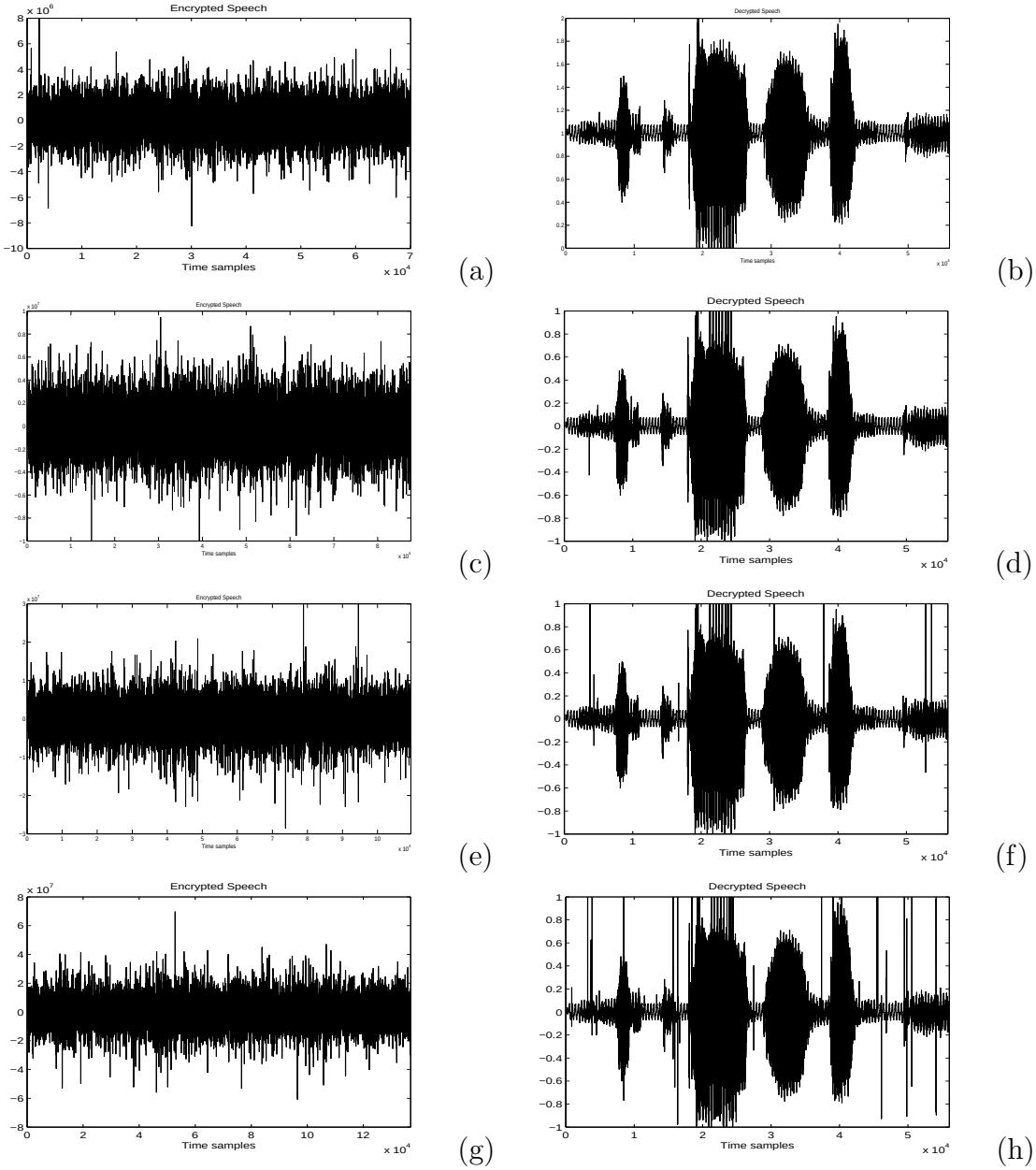


Figure 6.6: A comparison between cipher-texts and recovered signals for oblique and iterative oblique subspace-based speech encryption, (a)-(b) 1-round, (c)-(d) 2-rounds, (e)-(f) 3-rounds, (g)-(h) 4-rounds.

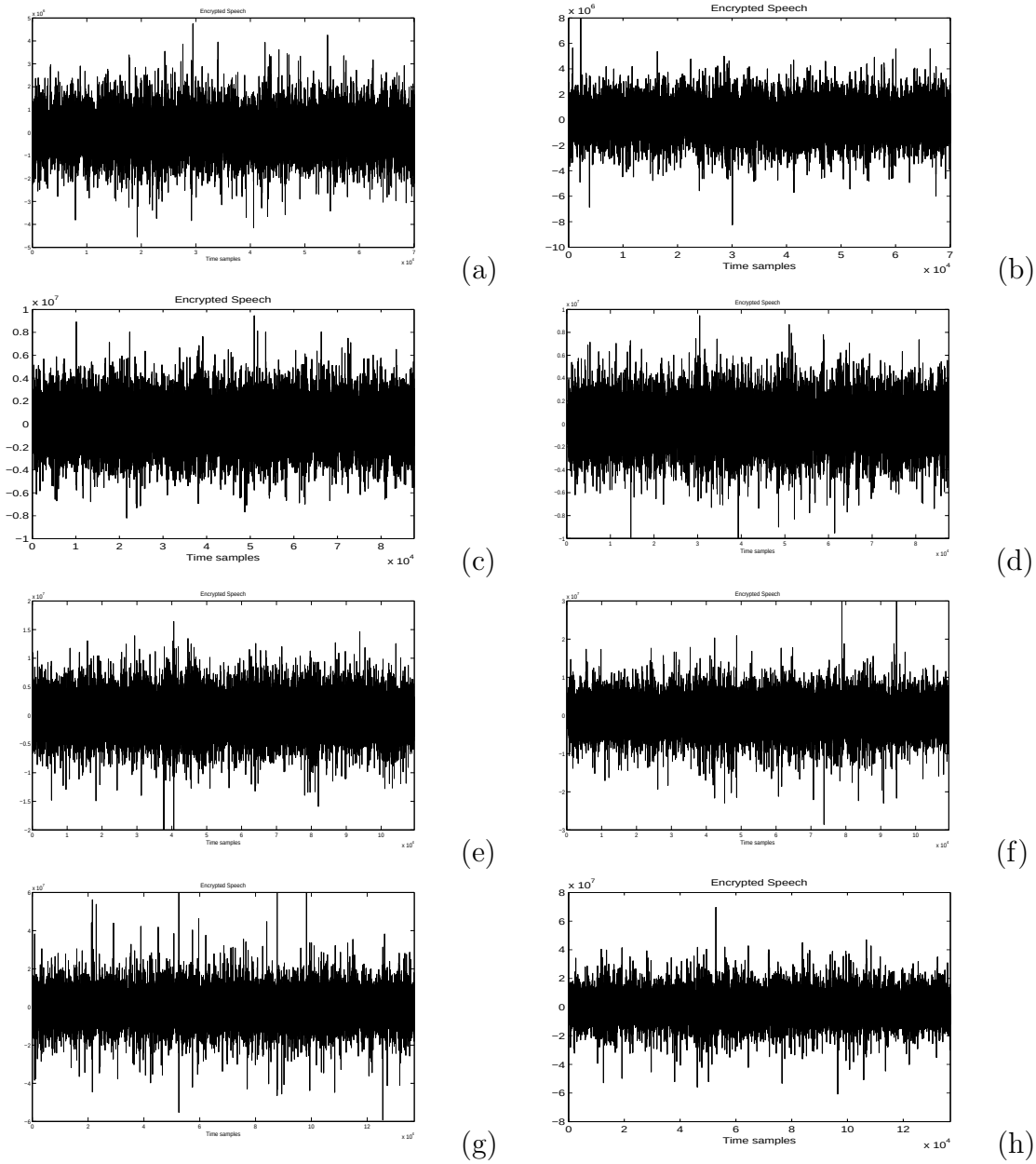


Figure 6.7: A comparison between cipher-texts for iterative orthogonal and iterative oblique subspace-based speech encryption, (a)-(c)-(e)-(g) 1, 2, 3 and 4-rounds orthogonal encryption, (b)-(d)-(f)-(h) 1, 2, 3 and 4-rounds oblique encryption.

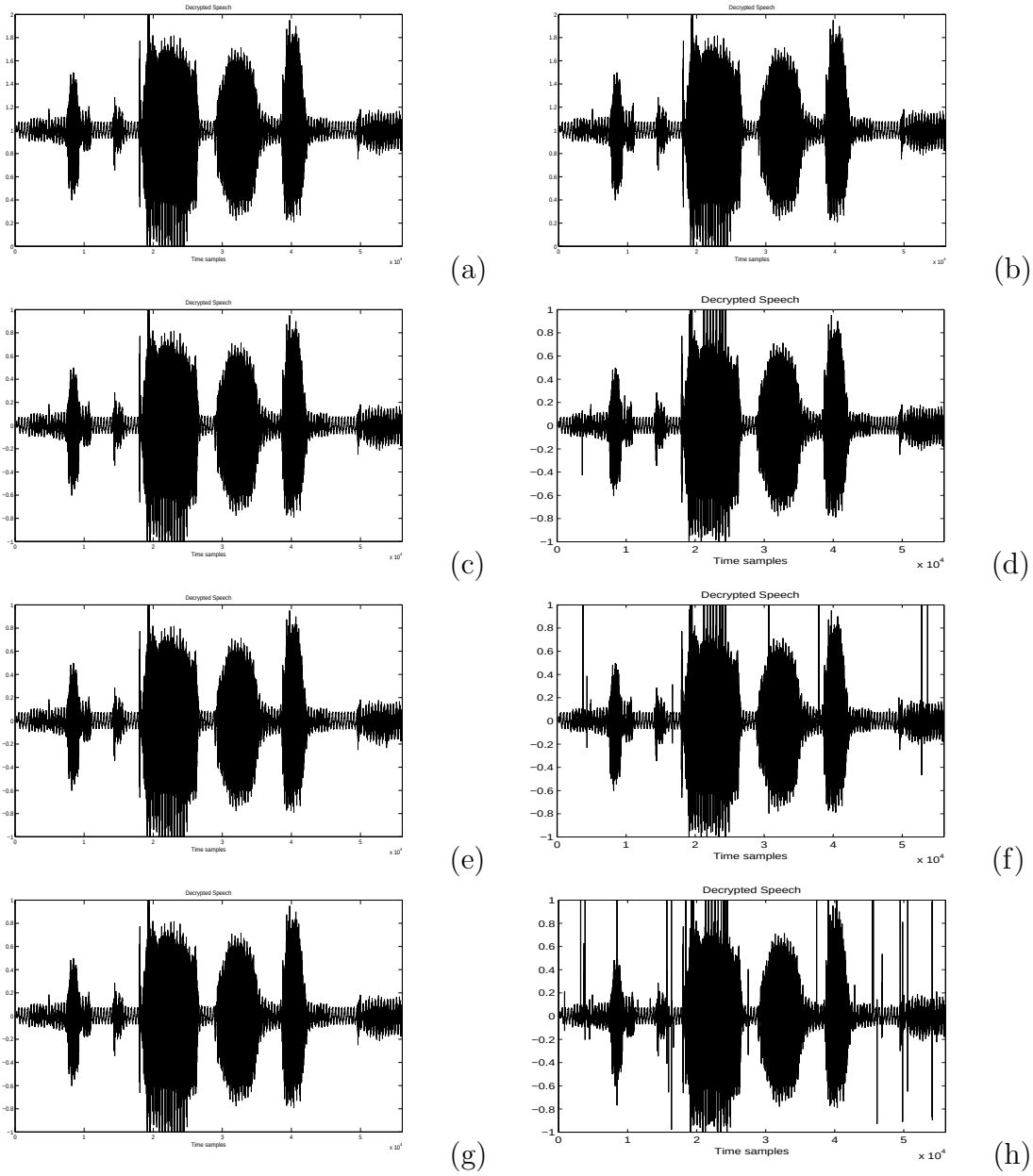


Figure 6.8: A comparison between recovered signals for iterative orthogonal and iterative oblique subspace-based speech encryption, (a)-(c)-(e)-(g) 1, 2, 3 and 4-rounds orthogonal encryption, (b)-(d)-(f)-(h) 1, 2, 3 and 4-rounds oblique encryption.

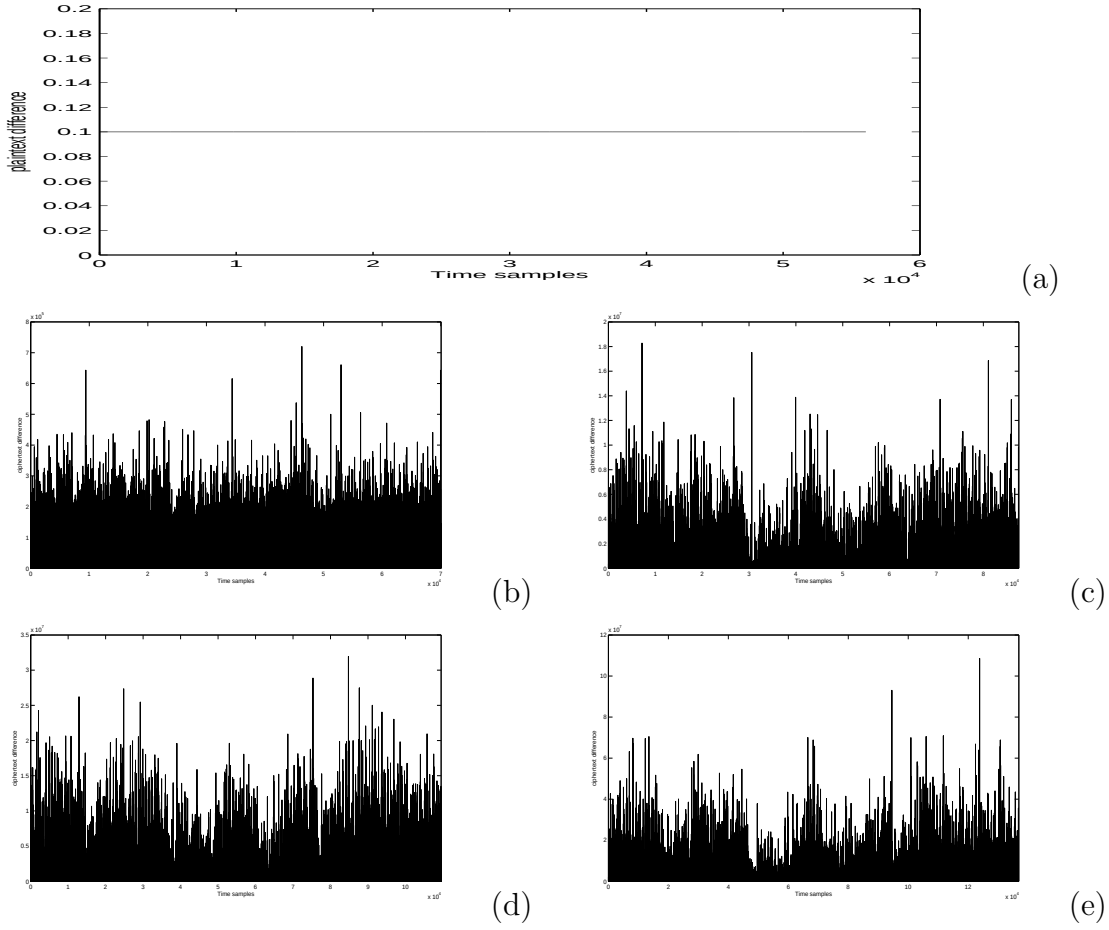


Figure 6.9: A comparison in terms of sensitivity levels to a 0.1 plain-text mismatch between iterative orthogonal subspace-based encryption schemes for different iterations, (a) plain-text mismatch, cipher-text difference for: (b) 1-round, (c) 2-rounds, (d) 3-rounds, (e) 4-rounds.

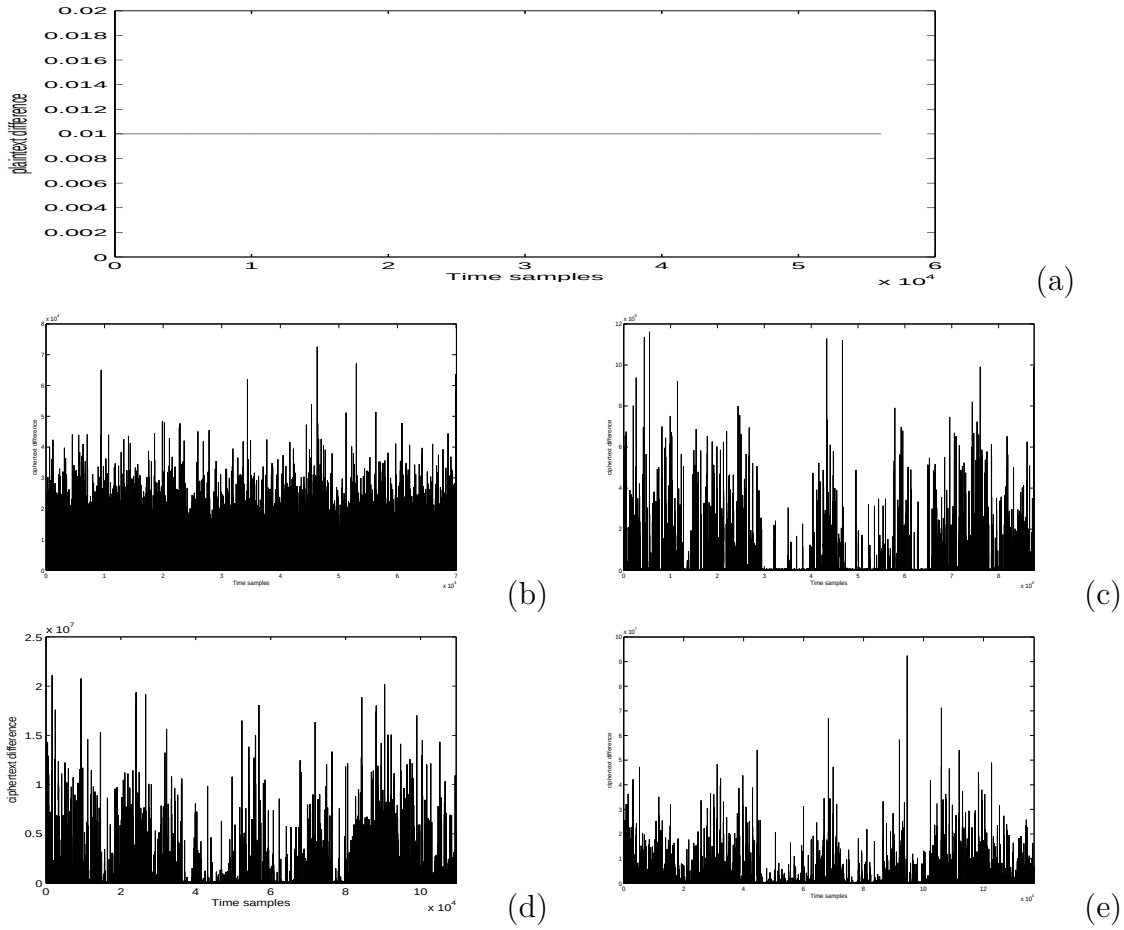


Figure 6.10: A comparison in terms of sensitivity levels to a 0.01 plain-text mismatch between iterative orthogonal subspace-based encryption schemes for different iterations, (a) plain-text mismatch, cipher-text difference for: (b) 1-round, (c) 2-rounds, (d) 3-rounds, (e) 4-rounds.

different iterations: 1-round, 2-rounds, 3-rounds and 4-rounds encryption. One can see that, for the same plain-text mismatch level, the sensitivity of the oblique-based encryption scheme is higher than the sensitivity of the orthogonal-based encryption scheme. This can be seen by comparing the obtained cipher-text difference level which also increases when the number of iterations rises.

In Figure (6.13)-(a), the experimental relationship between the recovery error and the value of mismatch level ϵ is plotted for different iterations when the iterative orthogonal subspace encryption is used. The value of the factor β is equal to 10^6 and the values of ϵ varie from 10^{-3} to 1. For the smallest value of ϵ used during experimentations, one can see that the corresponding recovery error expressed in terms of Mean Absolute Error (MAE) is high (10^4) for a 2-rounds encryption. However, for the same smallest value of ϵ, the recovery error rises to 10^5 for a 6-rounds encryption.

The second experimental relationship, between the recovery error and the value of the factor β for the iterative orthogonal encryption scheme is shown in Figure (6.13)-(b). One can see that there is a linear relationship between the factor β and the recovery error. For the same value of β, let us say 10^6, the recovery error varies from 10^4 to 10^5 when the number of iterations varies from 2 to 6.

Figure (6.14)-(a) shows a plot of the experimental relationship between the recovery error and the value of mismatch level ϵ for different iterations when the iterative oblique subspace encryption is used. The values of ϵ varie from 10^{-3} to 1 and the value of the factor β is equal to 10^6. One can see that the recovery error expressed in terms of Mean Absolute Error (MAE) is high (10^3) for a 10^{-3} value of ϵ when we apply a 2-rounds encryption. However, for the same value of ϵ, the recovery error rises to reach a level of 10^9 for a 6-rounds encryption.

Then, the experimental relationship between the recovery error and the value of the factor β for the iterative oblique encryption scheme is shown in Figure (6.14)-(b). One can see that there is roughly a linear relationship between the factor β and the recovery error. For the same value of β, let us say 10^6, the recovery error varies from 10^3 to 10^9 when the number of iterations varies

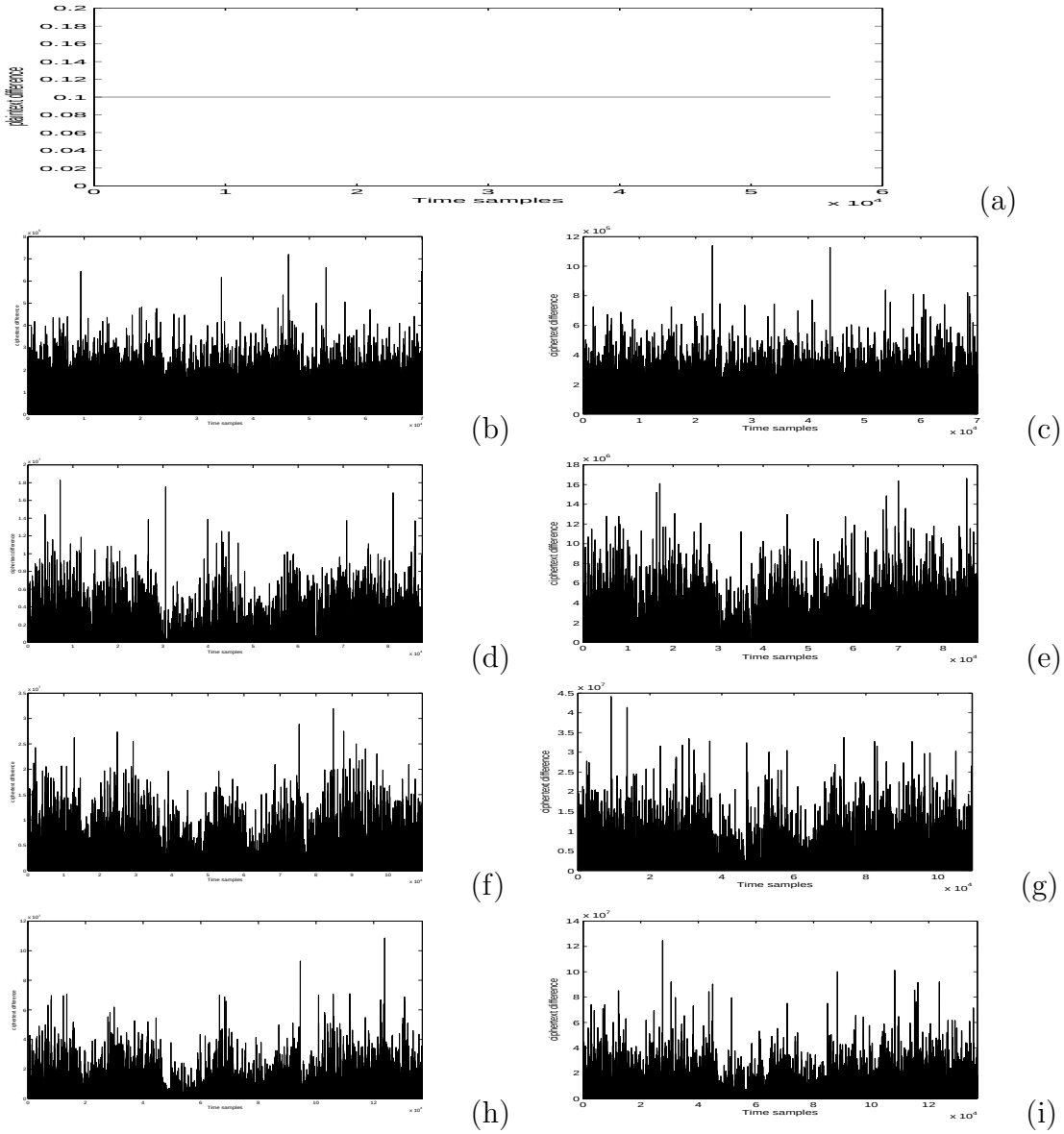


Figure 6.11: A comparison in terms of sensitivity levels to a 0.1 plain-text mismatch between iterative orthogonal and iterative oblique subspace-based encryption schemes for different iterations, (a) plain-text mismatch, (b)-(d)-(f)-(h) 1, 2, 3 and 4-rounds orthogonal encryption, (c)-(e)-(g)-(i) 1, 2, 3 and 4-rounds oblique encryption.

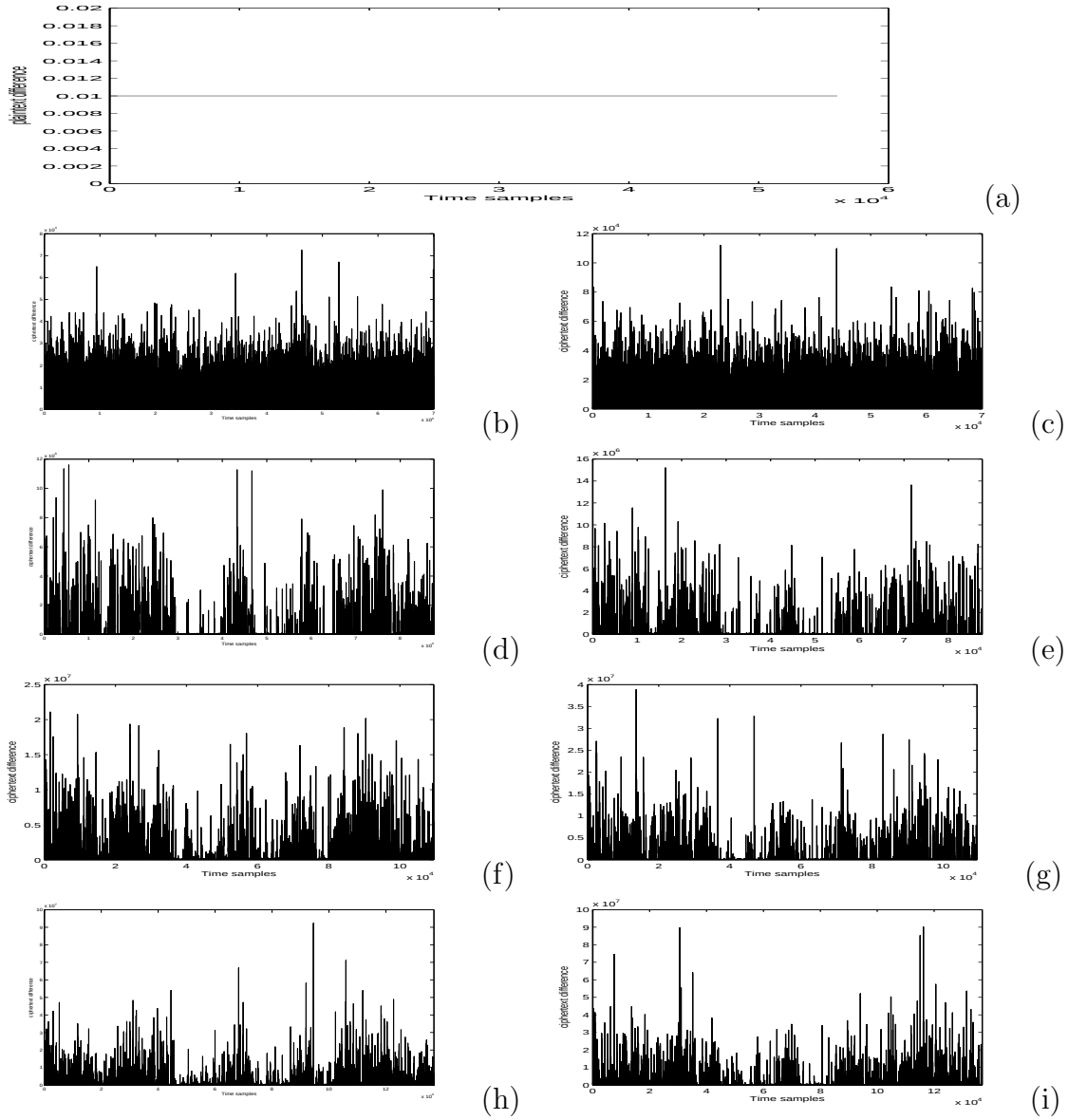
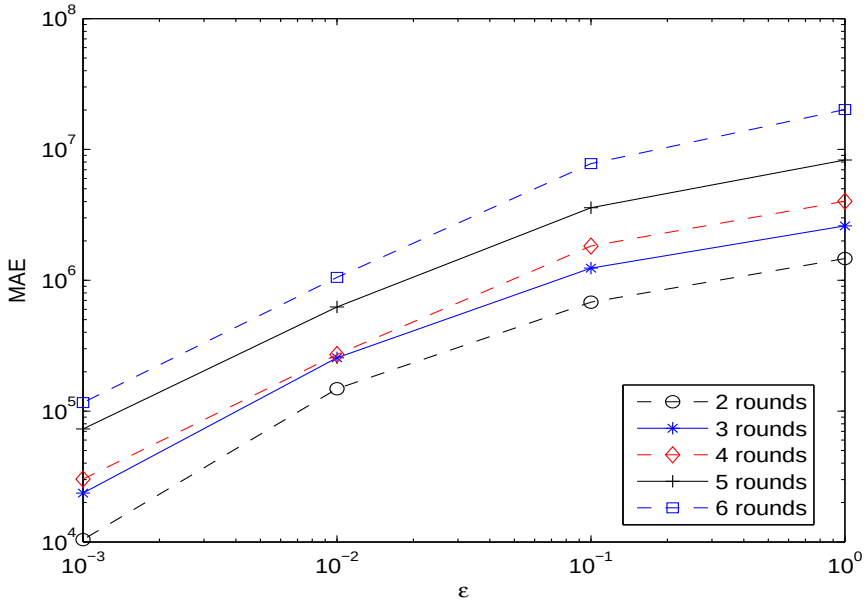
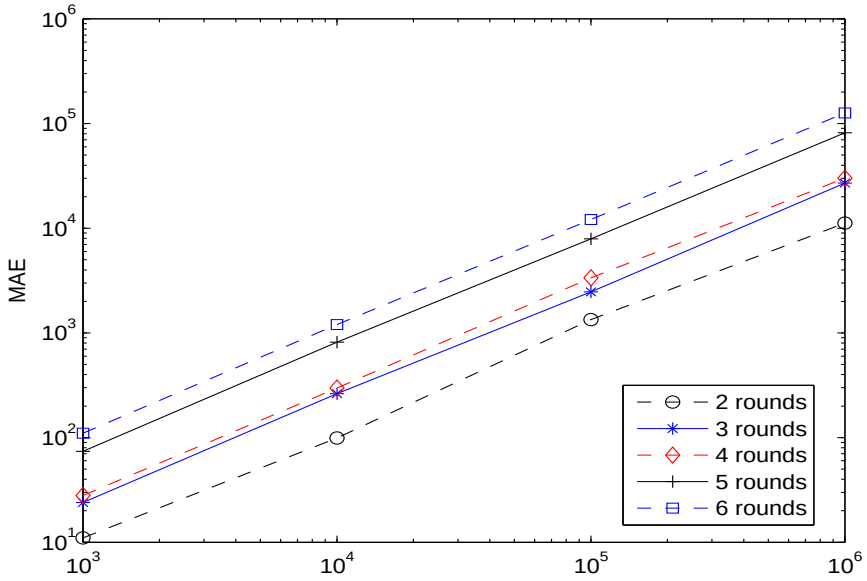


Figure 6.12: A comparison in terms of sensitivity levels to a 0.01 plain-text mismatch between iterative orthogonal and iterative oblique subspace-based encryption schemes for different iterations, (a) plain-text mismatch, (b)-(d)-(f)-(h) 1, 2, 3 and 4-rounds orthogonal encryption, (c)-(e)-(g)-(i) 1, 2, 3 and 4-rounds oblique encryption.

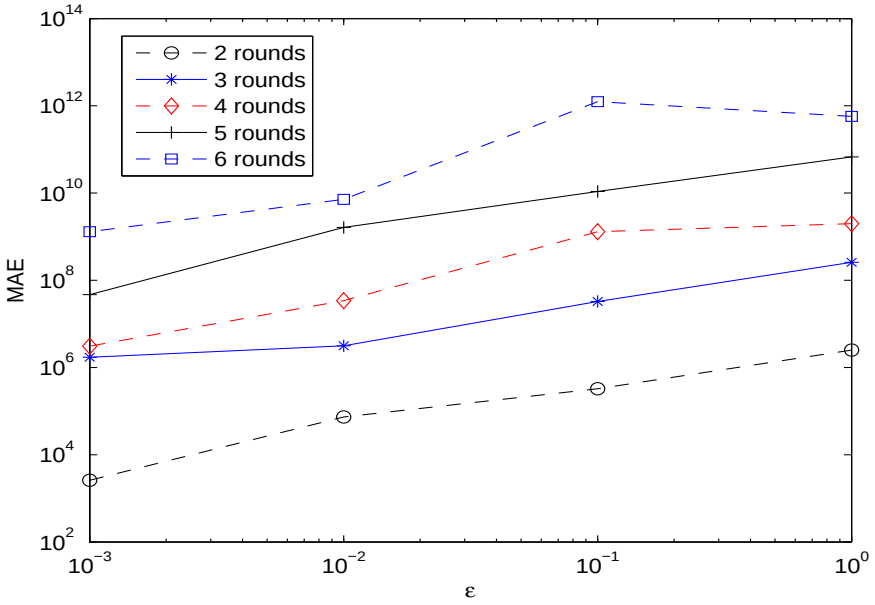


(a)

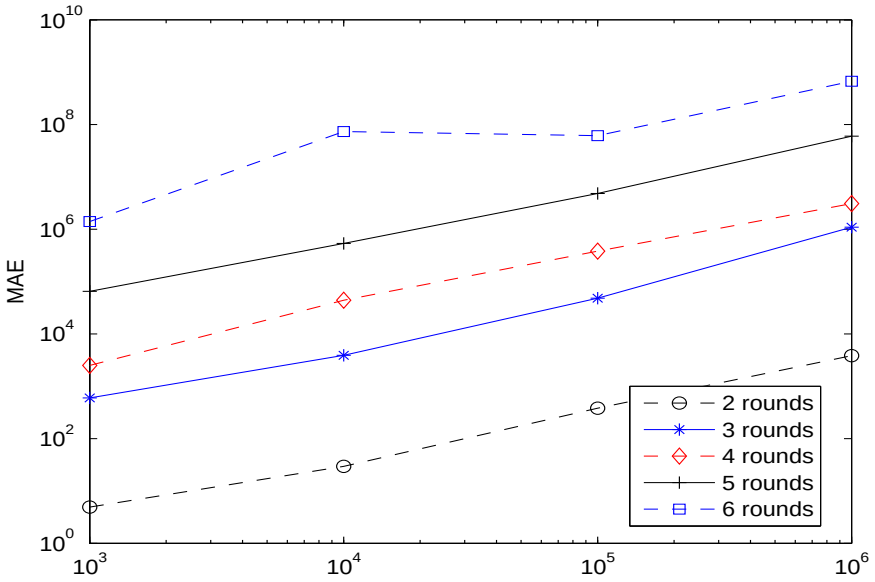


(b)

Figure 6.13: The experimental relationship, in speech encryption, between the recovery error and the value of ϵ and β for different rounds in the iterative orthogonal subspace encryption scheme, (a) $\beta = 10^6$, (b) $\epsilon = 0.001$.



(a)



(b)

Figure 6.14: The experimental relationship, in speech encryption, between the recovery error and the value of ϵ and β for different iterations in the iterative oblique subspace encryption scheme, (a) $\beta = 10^6$, (b) $\epsilon = 0.001$.

from 2 to 6.

As a comparison between the above mentionned experimental relationships, of both iterative orthogonal and iterative oblique encryption schemes, one can see that the initial level of recovery error is higher in the 2-rounds iterative orthogonal scheme than in the 2-rounds iterative oblique scheme for the same values of β and ϵ. However, starting from a 3-rounds encryption, this recovery error level rises quickier to reach higher levels in the itreative oblique scheme than in the iterative orthogonal scheme for the same values of β and ϵ.

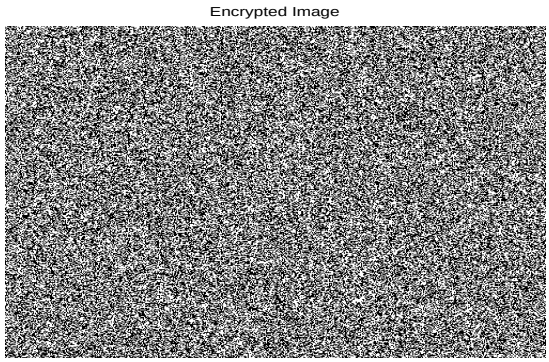
6.2 Application to image signal

Beside the speech application, the proposed subspace-based encryption scheme is applied on image. Figure (6.15) shows an example of this application. Figure (6.15)-(a), (b) and (c) show respectively the original image, the encrypted image and the decrypted one. As one can see, there is no distinguishable difference between the original and recovered images while the encrypted image is visually well protected.

Figures (6.16)-(a) and (6.16)-(b) show a comparison in terms of sensitivity levels to plain-text mismatches of respectively 0.1 and 0.01 when we apply orthogonal subspace-based encryption scheme on the image used previously. One can see that the sensitivity of the orthogonal-based encryption scheme, revealed by the cipher-text difference level, is at lower levels comparing to the speech application's case in terms of empirical measurements.

However, Figure (6.17) shows, visually, the high level of sensitivity of the orthogonal subspace-based encryption scheme when applied on an image. One can see that for a very small key mismatch, it is impossible to recover the original image. As it can be seen, the decrypted image looks like an encrypted one. In Figure (6.18), the experimental relationship between the recovery error and the value of mismatch level ϵ is plotted when orthogonal subspace-based scheme is used in image encryption for different iterations. The value of the factor β is equal to 10^6 and the values of ϵ varie from 10^{-3}

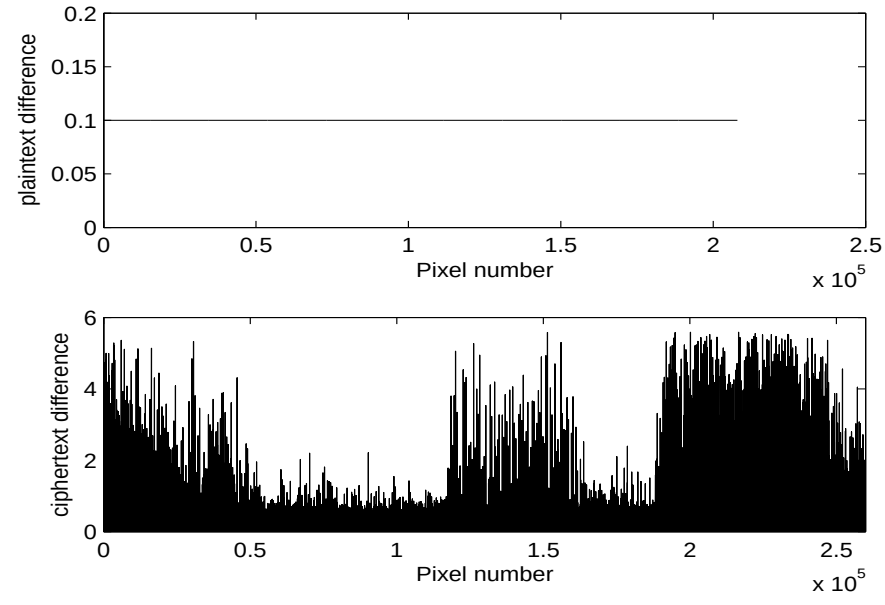
(a)



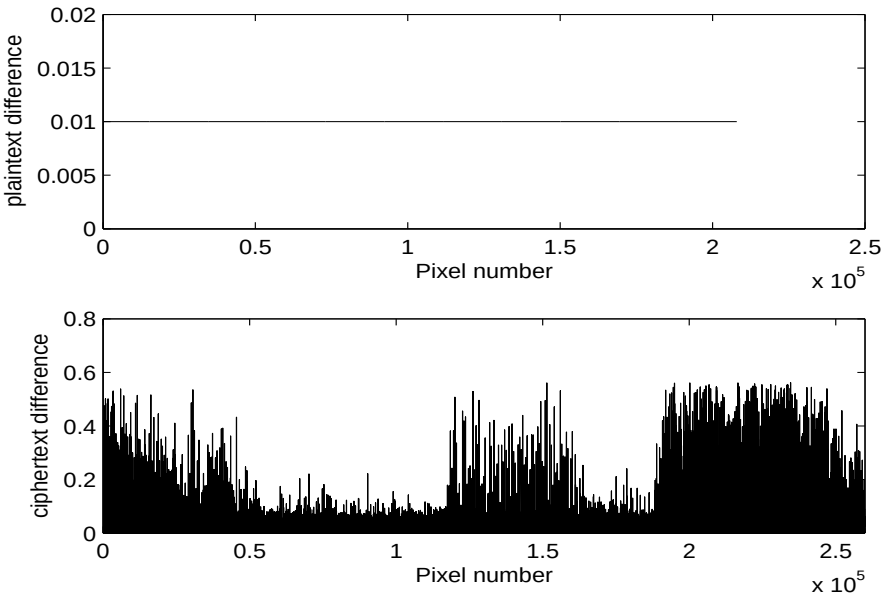
(b)

(c)

Figure 6.15: An example of orthogonal subspace-based image encryption, (a) Original image, (b) Encrypted image, (c) Decrypted image.



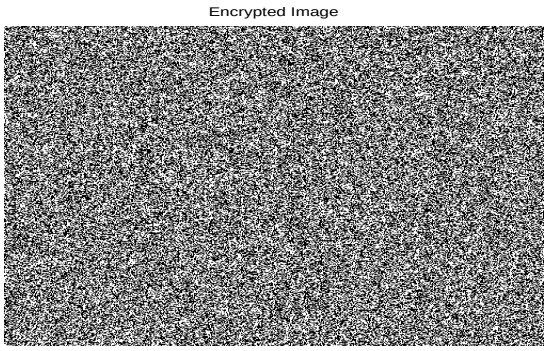
(a)



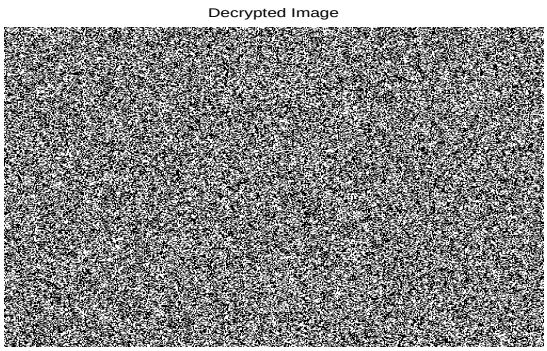
(b)

Figure 6.16: Sensitivity, in image encryption, to plain-text with $\beta = 10^6$ for, (a) $\epsilon = 0.1$, (b) $\epsilon = 0.01$.

(a)



(b)



(c)

Figure 6.17: An example of sensitivity of orthogonal subspace-based image encryption to a very small key mismatch, (a) Original image, (b) Encrypted image, (c) Decrypted image.

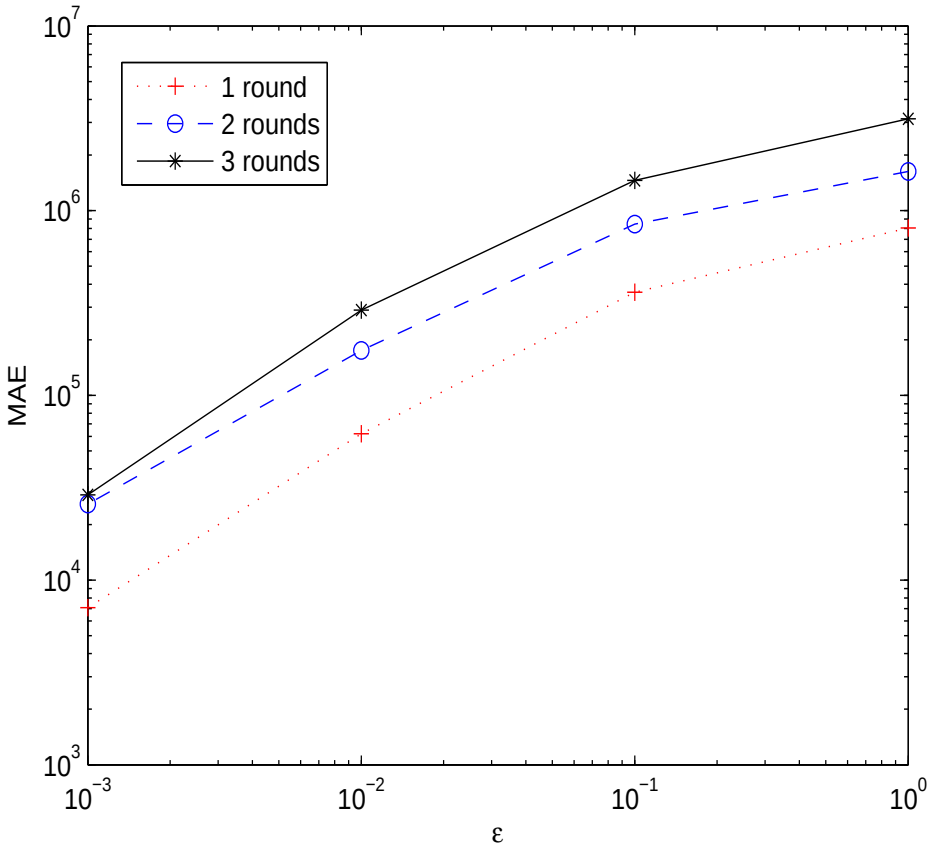


Figure 6.18: The experimental relationship in orthogonal subspace-based image encryption between the recovery error and the value of ϵ for $\beta = 10^6$.

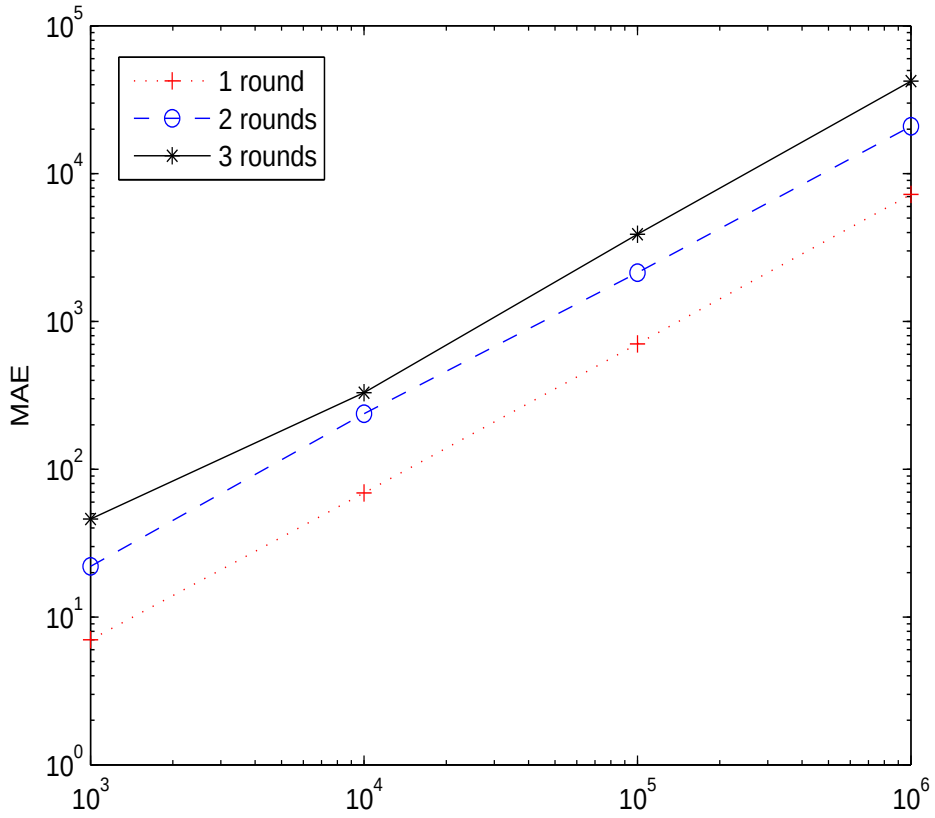


Figure 6.19: The experimental relationship, in orthogonal subspace-based image encryption, between the recovery error and the value of β for $\epsilon = 0.001$.

to 1. For the smallest value of ϵ, one can see that the corresponding recovery error is high (7×10^3).

The experimental relationship, between the recovery error and the value of the factor β when the orthogonal subspace-based scheme is used in image encryption, for different iterations, is shown in Figure (6.19). One can see that there is a linear relationship between the factor β and the recovery error.

However, Figure (6.20) shows the experimental relationship between the recovery error and the value of mismatch level ϵ when oblique subspace-based scheme is used in image encryption for 1 and 2 rounds. The value of the factor β is equal to 10^6 and the values of ϵ varie from 10^{-3} to 1. One can see the rise in the Mean Absolute Error (MAE) when we apply a second round for the same value of ϵ.

6.3 Application to binary phase shift keying (BPSK) data

Beside the speech and image applications, the proposed orthogonal subspace-based encryption scheme is applied on binary data. Figures (6.21) and (6.22) show an example of this application. Figure (6.21)-(a), (b) and (c) show respectively the original data, the encrypted data and the decrypted one. We see that the data are correctly recovered. Note that the encrypted data has more samples than the original one, actually L samples more where L is the segment number (100 in this example). This sample excess comes from the fact that the dimension of the key matrices $\mathbf{A}(t)$ is $(M+1) \times M$. Figure (6.22) shows the random key signal used during encryption process of binary data.

Figures (6.23)-(a) and (6.23)-(b) show a comparison in terms of sensitivity levels to plain-text mismatches of respectively 0.1 and 0.01 when we apply orthogonal subspace-based encryption scheme on binary data.

The experimental relationship between the recovery error and the value of mismatch level ϵ for different iterations when the iterative orthogonal subspace encryption is applied on binary data is shown in Figure (6.24)-(a).

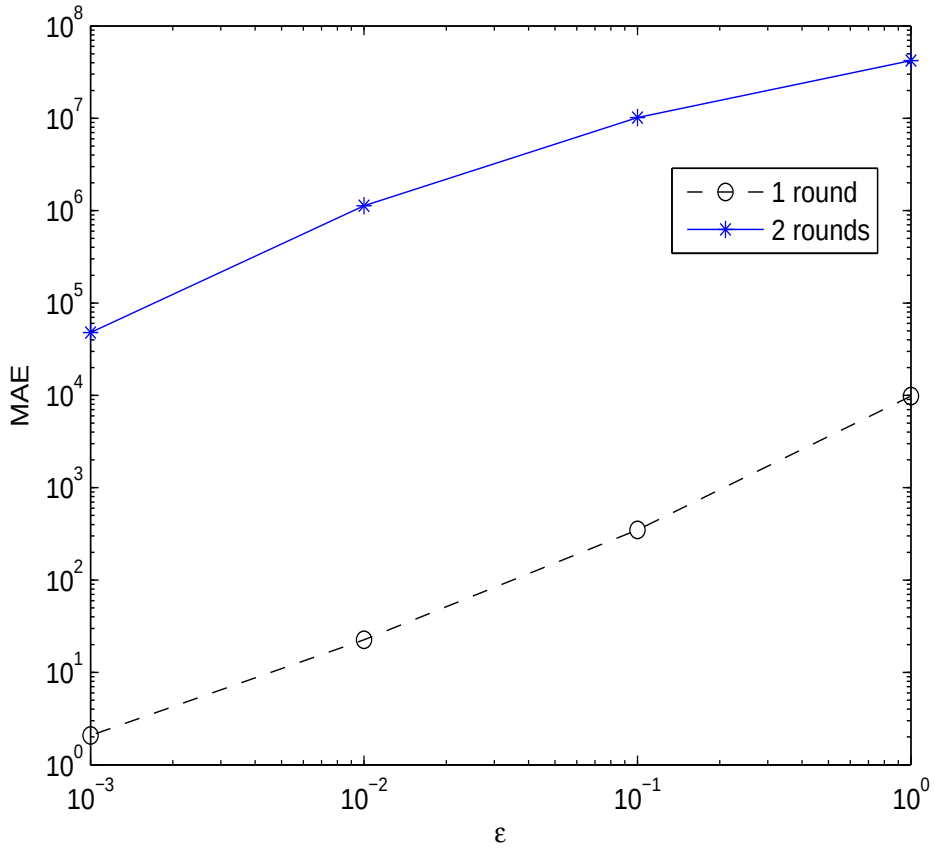
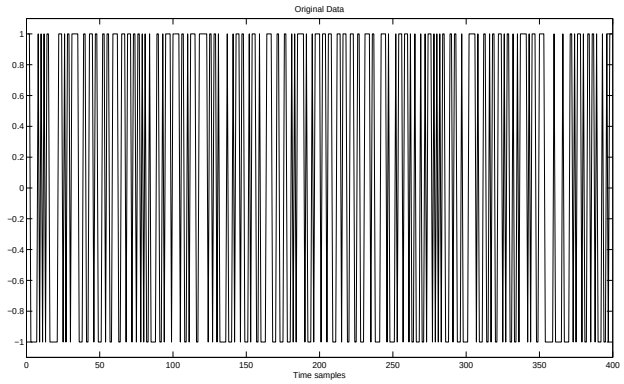
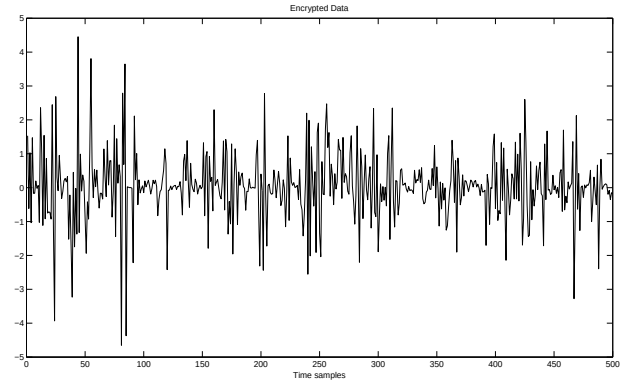


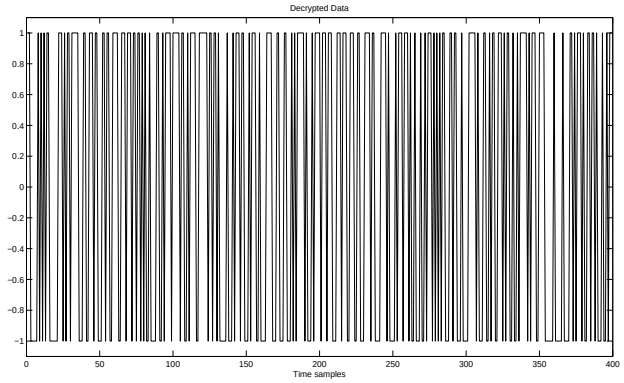
Figure 6.20: The experimental relationship, in oblique subspace-based image encryption, between the recovery error and the value of $\epsilon = 0.001$ for $\beta = 10^6$.



(a)



(b)



(c)

Figure 6.21: An example of orthogonal subspace-based BPSK data encryption, (a)Original data, (b) Encrypted data, (c) Decrypted data.

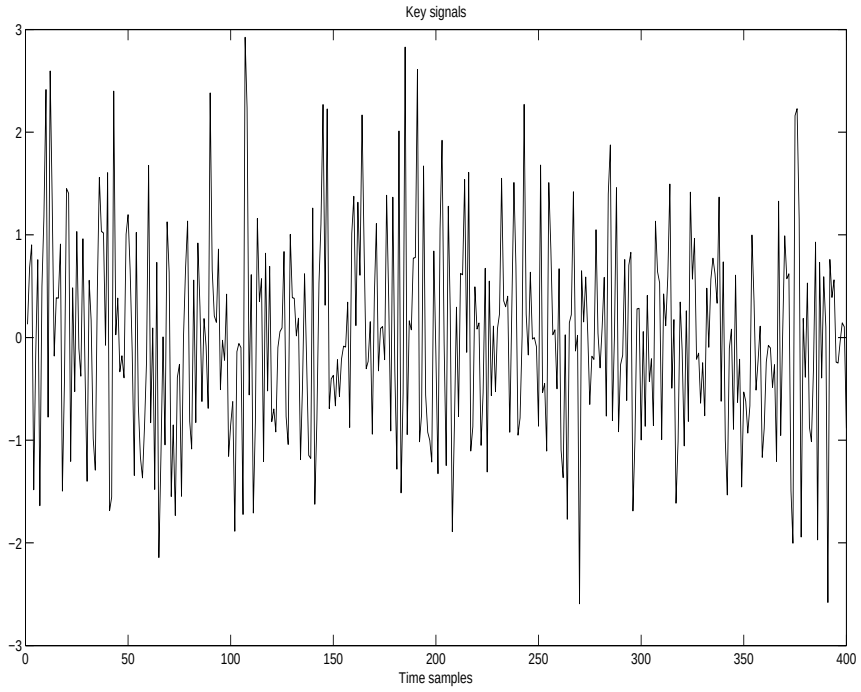
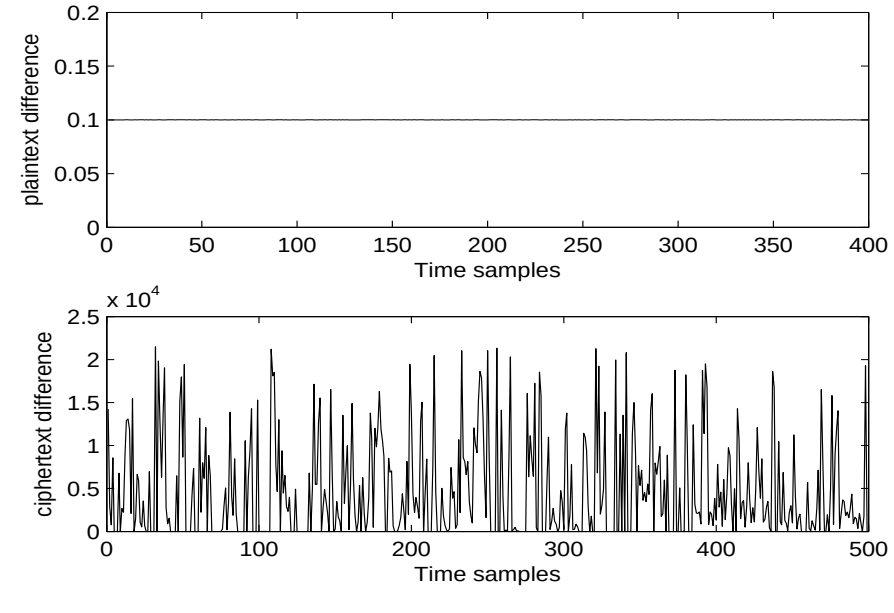
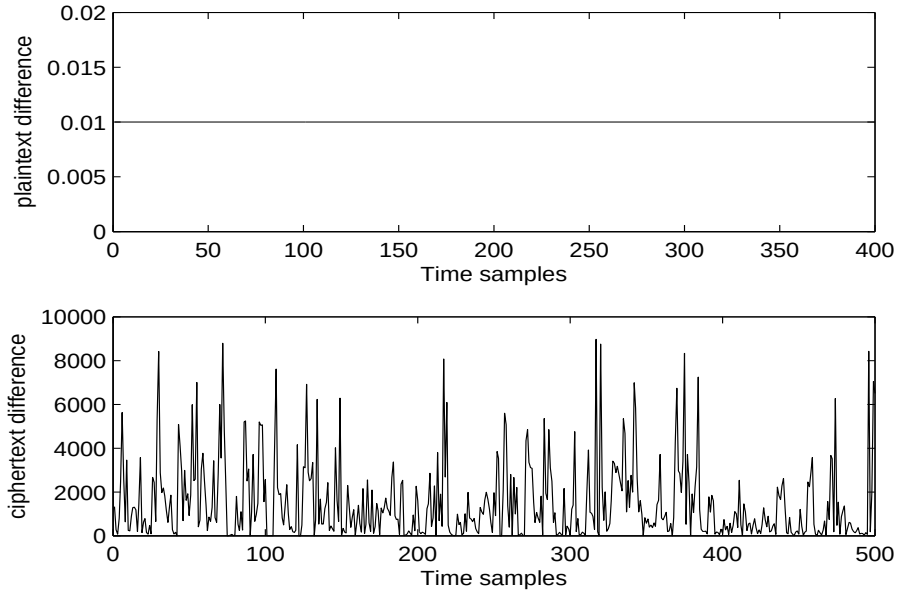


Figure 6.22: The key signal used in the example of the orthogonal subspace-based BPSK data encryption.



(a)



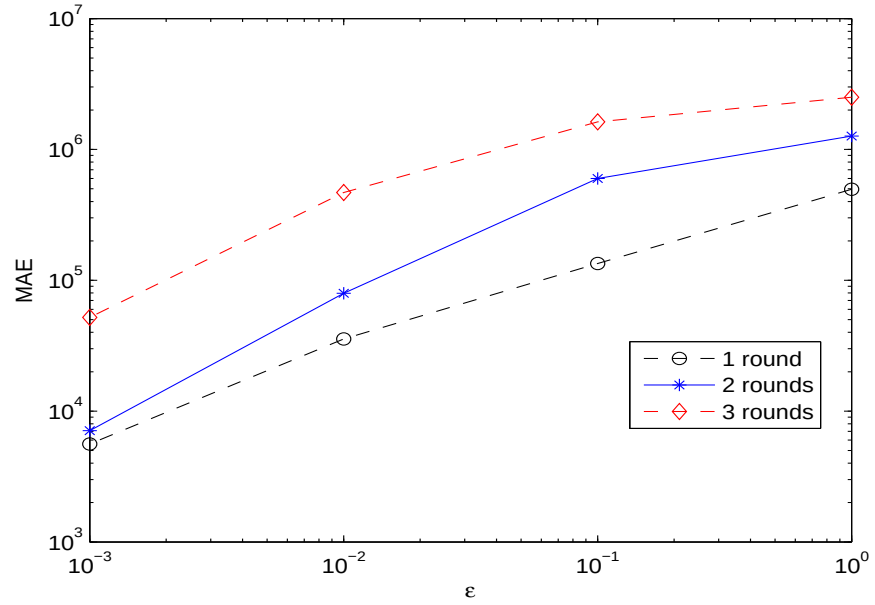
(b)

Figure 6.23: Sensitivity, in orthogonal subspace-based BPSK data encryption, to plain-text with $\beta = 10^6$ for, (a) $\epsilon = 0.1$, (b) $\epsilon = 0.01$.

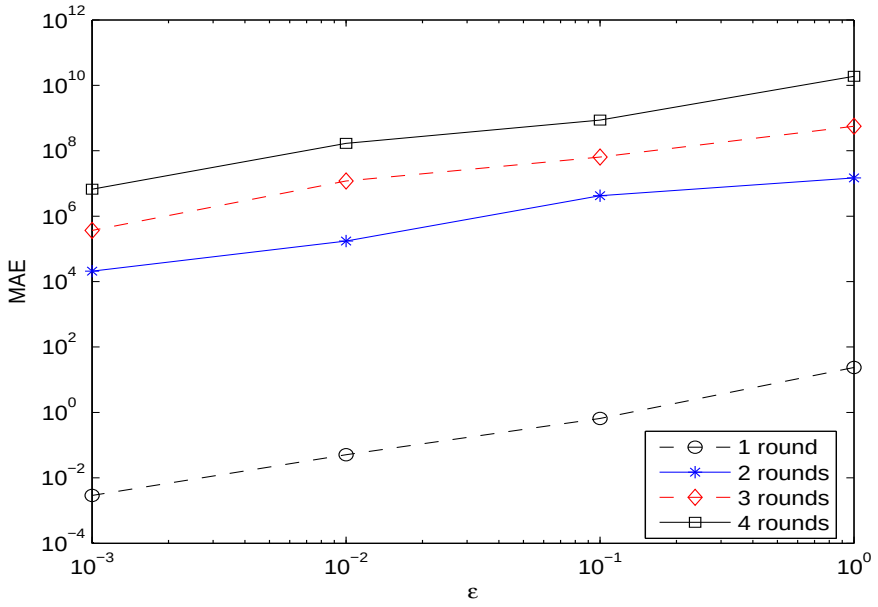
The values of ϵ varie from 10^{-3} to 1 and the value of the factor β is equal to 10^6. One can see that the recovery error expressed in terms of Mean Absolute Error (MAE) is high (5×10^3) for a 10^{-3} value of ϵ when we apply a 1-round encryption. However, for the same value of ϵ, the recovery error rises to reach a level of 5×10^4 for a 3-rounds encryption.

For the oblique approach, Figure (6.24)-(b) shows a plot of the experimental relationship between the recovery error and the value of mismatch level ϵ for different iterations. The values of ϵ varie from 10^{-3} to 1 and the value of the factor β is equal to 10^6. One can see that the recovery error expressed in terms of Mean Absolute Error (MAE) is low (10^{3-}) for a 10^{-3} value of ϵ when we apply a 1-round encryption. However, for the same value of ϵ, the recovery error rises to reach a level of 10^4 for only a 2-rounds encryption. One can see that the impact of applying a second round in this scheme is much more important than the impact of the other rounds.

As a comparison in terms of experimental between both iterative orthogonal and iterative oblique encryption schemes, one can see that the initial level of recovery error is higher in the 1-round iterative orthogonal scheme than in the 1-round iterative oblique scheme for the same value of ϵ. However, starting from a 2-rounds encryption, this recovery error level rises quickier to reach higher levels in the iterative oblique scheme than in the iterative orthogonal scheme for the same value ϵ.



(a)



(b)

Figure 6.24: The experimental relationship between the recovery error and the value of ϵ for different iterations when applied to BPSK data, (a) iterative orthogonal subspace scheme, (b) iterative oblique subspace scheme.

Chapter 7

Conclusion

In this thesis, an investigation of the opportunity of using techniques based on the subspace concept in the encryption field is conducted. First, the investigation starts with studying blind source separation (BSS) techniques and their application in the encryption domain. Analysis of the robustness characteristics of some BSS-based encryption techniques shows weaknesses from a crytpographic point of view.

Then, a new approach based on the subspace concept is presented in order to bypass the above weaknesses. The first approach presented in this thesis is based on orthogonal subspace technique then applied in speech, image and data encryption. The second approach is based on oblique subspace technique and is also applied for speech, image and data encryption.

For both orthogonal and oblique subspace-based encryption approachs, iterative versions are developped and applied for speech, image and data encryption. The need for iterations is a known issue in the design of cryptographic algorithms. In our proposed subspace-based encryption algorithm, this need is motivated by the added-value, from a cryptographic robustness point of view, provided by the application of successive iterations. Of course, iterations do not have an impact on the quality of recovering the original plain-text.

On another hand, several simulations and tests are conducted to evaluate the robustness of the subspace-based schemes presented in this thesis. That is why, crytpanalysis techniques are used to appreciate and to evaluate this

robustness. Experimental results and discussion confirm an enhancement in security level with respect to BSS-based encryption techniques. These results show a new direction, for using non-classical approach in encryption domain, inspired from digital signal processing field.

Originality of the thesis contributions

The originality of the thesis contributions consists of the following added values:

- The judicious choice of the second term of equation (3.2) which describes the encryption operations. This term is made as complicated as possible to not be recovered or attacked by the cryptanalysis techniques used against blind source separation-based encryption schemes. This additive term is nonlinear and correlated with the first term of the encryption procedure.

- The proposed subspace-based encryption scheme provides no cipher-text at the output if there is no plain-text at the input i.e. the cipher-text vanishes if there is no plain-text provided. To our knowledge, this problem has no solution yet from a statistical signal processing point of view.

- Only a part of the cryptographic keys used in the procedure of encryption is necessary for decryption. The proposed subspace technique provides the ability to have this interesting feature.

- The cipher-texts obtained after encrypting the same plain-text using the same key matrix in the proposed subspace encryption scheme are totally different. This feature represents an enhancement in the resistance to cipher-text-only cryptanalysis attack. The uncertainty about the exact number of plain-texts corresponding to a number of collected cipher-texts represents a considerable constraint at the beginning itself of a cryptanalysis attack and consequently constitutes, from a security

point of view, an important feature of our proposed system.

- The key space provided by the key matrix is huge because of the generation of a key matrix for each cipher-text vector. The high sensitivity of the proposed subspace-based encryption scheme to key matrix ensures that this mixing matrix cannot be approxiamtely guessed under a relatively large finite precision ϵ.

- The iterative subspace-based encryption scheme gives better results, from a cryptographic robustness point of view, than the one-iteration subspace scheme. This is due to the accumulation, provided by the successive iterations, of the basic security characteristics of the proposed subspace-based encryption method. Of course, the iterations have a cost in terms of processing speed. A compromise, depending on the requirements of the target field of application of the subspace-based encryption scheme, has to be found between the number of iterations and processing speed.

- The oblique subspace encryption approach provides an enhancement of the results, from a cryptographic robustness point of view, already achieved by the orthogonal subspace approach.

- Confusion and diffusion are the two most important security requirements for a cryptographic system. While in most of the published cryptographic systems, confusion and diffusion are guaranteed through the application mainly of substitution and permutation operators, our proposed subspace-based approach provides the same security objectives but differently. Confusion which consists of obscuring the relationship between the plain-text, the cipher-text and the key is achieved through the linearity and the nonlinearity existing in the subspace-based encryption procedure. Diffusion is achieved through creating a tight dependency of each value of the cipher-text on each value of the plain-text and each value of the key.

- During the design of the subspace-based encryption scheme, a special attention has been given beside the security robustness and quality of recovered signals, to ease of use and to the ability to achieve hardware implementation later (hardware implementers are more important than cryptographers). Because of hardware implementation requirements, the decryption scheme could not be an inverse operation of the encryption scheme i.e. one could not apply a hardware backward process (transistors do not allow a current return), it is recommended to make the decryption scheme the most comparable, in hardware sense, to the encryption one.

  At this step, the subspace-based decryption scheme does not require a backward process, rather it applies the same approach by projecting the cipher-text (encrypted signal) on a subspace. Of course, the calculation of the pseudo-inverse of a matrix to recover the original signal remains an issue for future optimization of our proposed scheme in order to give the best conditions for hardware implementations.

Bibliography

[1] H. Delfs and H. Knebl, "Introduction to cryptography : principles and applications", Berlin : Springer-Verlag, 2002.

[2] A. Belouchrani, K. A. Meraim, J.-F. Cardoso, and E. Moulines, "A blind source separation technique using second-order statistics," in IEEE Trans. Signal Processing, vol. 45, no. 2, pp. 434-444, February 1997.

[3] A. Belouchrani, and M. Amin, "Blind source separation based on time-frequency signal representations," in IEEE Trans. Signal Processing, vol. 46, no. 11, pp. 2888-2897, November 1998.

[4] Q.-H. Lin, and F.-L. Yin "Blind source separation applied to image cryptosystems with dual encryption ," in Electronics Letters, vol. 38, no. 19, pp. 1092-1094, September 2002.

[5] Q.-H. Lin, F.-L. Yin, and Y.-R. Zheng "Secure image communication using blind source separation," in IEEE 6th CAS Symp. on Emerging Technologies: Mobile and Wireless CO. Shanghai, China, May 31-June 2, 2004.

[6] Q.-H. Lin, F.-L. Yin, T.-M. Mei, and H.-L. Liang, "A speech encryption algorithm based on blind source separation," in Proc. Int. Conf. Commun., Circuits Syst.: Signal Process., Circuits Syst., 2004, vol. II, pp. 1013-1017.

[7] Q.-H. Lin, F.-L. Yin, T.-M. Mei, and H. Liang, "A blind source separation based method for speech encryption," in IEEE Trans. Circuits Syst. I, vol. 53, no. 6, pp. 1320-1328, June 2006.

[8] Q. Lin and F. Yin, "Image cryptosystems based on blind source separation," in Proceedings of the 2003 International Conference on Neural

Networks and Signal Processing (ICNNSP2003), vol. 2. IEEE, 2003, pp. 1366-1369.

[9] Q. Lin, F. Yin, and H. Liang, "Blind source separation-based encryption of images and speeches," in Advances in Neural Networks - ISNN 2005 Proceedings, Part II, ser. Lecture Notes in Computer Science, vol. 3497. Berlin / Heidelberg: Springer-Verlag, 2005, pp. 544-549.

[10] Q.-H. Lin, F.-L. Yin, and H.-L. Liang, "A fast decryption algorithm for BSS-based image encryption, in Advances in Neural Networks - ISNN 2006 Proceedings, Part III, ser. Lecture Notes in Computer Science, vol. 3973. Berlin / Heidelberg: Springer-Verlag, 2006, pp. 318-325.

[11] S. Li, C. Li, K.-T. Lo, and G. Chen, "Cryptanalyzing of an encryption scheme based on blind source separation," in IEEE Trans. Circuits Syst. I, vol. 55, no. 4, pp.1055-1063, 2008.

[12] A. Mermoul and A. M. Absi, "On the relationship between research and community needs among the Arab-Muslim civilization heritage: an example in cryptology", in Proc. International Forum on Engineering Education. Sharjah, U.A.E, February, 2006.

[13] M. Merayati, Y. M. Alam and M. H. Attayane, Cryptography and Cryptanalysis among Arabs, Publications of the campus of the Arab language, Damascus, 1987, pp.39-40.

[14] C.E. Shannon, "Communication theory of secrecy systems, Bell system technical journal, vol. 28, pp. 656-715, Oct. 1949.

[15] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Trans. on Info. Theory, vol. IT-22, pp. 644-654, November 1976 (Invited Paper).

[16] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, Issue 2, pp. 120-126, February 1978, NY, USA.

[17] B. Schneier, "Applied crytpography : protocols, algorithms and source code in C", 2nd edition. New York: John Wiley & Sons, Inc., 1996, p.758.

[18] National Institute of Standards and Technology (US), "Specification for the advanced encryption standard (AES)", Federal Information Processing Standards Publication 197 (FIPS PUB 197), November 2001.

[19] John Paul Walters, Zhenggiang Liang, Weisong Shi, and Vipin Chaudhary, "Wireless Sensor Network Security: A Survey, 2006. (From Technical Report, December 2007 Security in Distributed Embedded Systems Masters thesis in Computer Systems Presented by Rohit Tewatia)

[20] C. Swenson, "Modern Cryptanalysis: Techniques for Advanced Code Breaking", New Jersey: Wiley, 2008.

[21] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig, "The Sybil Attack in Sensor Networks: Analysis Defenses, ISPN04, April 2004, California, USA. (From Technical Report, December 2007 Security in Distributed Embedded Systems Masters thesis in Computer Systems Presented by Rohit Tewatia)

[22] A. Mermoul, "Side Channel Attacks on Cryptographic Implementations", 1^{st} International Symposium on Electromagnetism, Satellites and Cryptography, Jijel, Algeria, 19-21 Jul. 2005.

[23] D. Kahn, The Code Breakers, 2^{nd} edition, McGraw-Hill, Inc., New York, pp. 80-81, 1973.

[24] P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," Advances in Cryptology - CRYPTO '96 Proceedings, Springer-Verlag, 1996, pp. 104-113.

[25] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis: Leaking Secrets", Advances in Cryptology - Proceedings of Crypto 99, Springer Verlag, LNCS 1666, pages 388397.

[26] K. Gandolfi, C. Mourtel, and F. Olivier, Electromagnetic analysis: Concrete results, Proc. of Cryptographic Hardware and Embedded Systems (CHES 2001) (çetin Kaya Koç, David Naccache, and Christof Paar, eds.), Lecture Notes in Computer Science, vol. 2162, Springer, 2001, pp. 251-261.

[27] D. Agrawal, B. Archambeault, S. Chari, J. R. Rao and P. Rohatgi, "Advances in side channel cryptanalysis: Electormagnetic analysis and

Template attacks," RSA Laboratories Cryotobytes, vol. 6, N° 1, pp. 20-32, 2003.

[28] NACSIM 5000: Tempest Fundamentals, National Security Agency, Fort George G.Meade, Maryland. Feb. 1982. Partially declassified also available at http://cryptome.org/nacsim-5000.htm.

[29] N. P. Smart, "Physical side-channel attacks on cryptographic systems", http://citeseerx.ist.psu.edu

[30] A. Belouchrani and J.F. Cardoso, "A maximum likelihood source separation for discrete sources", in Proc. EUSIPCO, vol. 2, pp. 768-771, September 1994.

[31] A. Taleb and C. Jutten, "On underdetermined source separation", in Proc. IEEE International Conference on Acoustics,Speech, Signal Processing (ICASSP 99), vol. 3, pp. 14451448, Phoenix, Ariz, USA, March 1999.

[32] D. Aissa EL Bey, K. Abed-Meraim, A. Belouchrani and Y. Grenier, "Underdetermined Blind Separation of Nondisjoint Sources in the Time-Frequency Domain", IEEE Trans. on Signal processing, vol. 55, Issue 3, pp. 897-907, March 2007.

[33] W. Kasprzak and A. Cichocki, "Hidden image separation from incomplete image mixtures by independent component analysis," in Proc. 13th Int. Conf. Pattern Recogn.,1996, vol. II, pp. 394-398.

[34] IEEE Computer Society, "IEEE standard for binary floating-point arithmetic," ANSSI/IEEE Std. 754-1985, 1985.

[35] R. Anderson, "Security Engineering - A guide to building dependable distributed systems". New York : John Wiley & Sons, Inc., 2001.

[36] P. Gutman, "Cryptographic security architecture : design and verification". New York : Springer-Verlag, 2004.

[37] O. Goldreich, "Modern cryptography, probalistic proofs and pseudorandomness". Berlin : Springer-Verlag, 1999.

[38] B. Sklar, "Digital communications : fundamentals and applications". New Jersey: Prentice-Hall Intenational, Inc., 1988.

[39] J. Soto, "Statistical Testing of Random Number Generators"' available at http://csrc.nist.gov/groups/ST/toolkit/rng/documents/nissc-paper.pdf

[40] U. Maurer, "A Universal Statistical Test for Random Bit Generators," Journal of cryptology, vol.5, PP. 89-105, 1992.

[41] Rémy Boyer and Guillaume Bouleux, "Oblique projections for direction of a arrival estimation with Prior Knowledge", IEEE Transaction on Signal Processing, Vol. 56, No. 4, April 2008

[42] R.Beherens and L.Sharf, "Signal processing Applications of oblique Projection Operator", IEEE trans. On Signal Processing, Vol. 42, No. 6, pp.1413-1424, June 1994.

[43] F. Mirza, "Block ciphers and cryptanalysis," available at http://fmirza.seecs.nust.edu.pk (2012).

[44] C. Cid, S. Murphy, M. Robshaw "Algebraic Aspects of the Advanced Encryption Standard," New York: Springer, 2006.

[45] ITU, "Methods for Subjective Determination of Transmission Quality", 1996, ITU-T Rec. P.800.

Appendix A

Publications

- A. Mermoul and A. M. Absi, "On the Relationship Between Research and Community Needs Among the Arab-Muslim Civilization Heritage: An Example in Cryptology", 4^{th} International Forum on Engineering Education: Integrating of Teaching and Research with Community Service, Sharjah, U.A.E., 25-27 Apr. 2006.
- A. Mermoul and A. Belouchrani, "A Subspace-based Method for Speech Encryption", in Proceedings of the 10^{th} International Conference on Information Science, Signal Processing and their Applications (ISSPA), pp. 538-541, Kuala Lumpur, Malaysia, 10-13 May 2010.
- A. Mermoul and A. Belouchrani, "An Image Encryption Method based on Subspace Techniques", $5^{ème}$ Séminaire sur les Systèmes de Détection: Architectures et Technologies DAT11, Alger, Algérie, 21-23 Fév. 2011.
- A. Mermoul, "An Iterative Speech Encryption Scheme based on Subspace Technique", in Proceedings of the 7^{th} International Workshop On Systems, Signal Processing and their Applications (WOSSPA), pp. 361-364, Tipaza, Algeria, 09-11 May 2011.
- A. Mermoul and A. Belouchrani, "Subspace-Based Technique for Speech Encryption", Digital Signal Processing, vol. 22, issue 2, pp. 298-303, Mar. 2012.

Appendix B

Filed Patent

– A. Mermoul et A. Belouchrani, "Procédé de chiffrement et déchiffrement de données et de signaux exploitant des techniques de sous espaces", INAPI, no. 080776, Déc. 2008.

Appendix C

Résumé

Introduction

Le développement rapide des communications et des échanges de données électroniques fait de la sécurité de l'information un enjeu crucial dans l'industrie, le commerce et l'administration. La cryptographie moderne propose des techniques essentielles pour garantir l'information et la protection des données. Les méthodes basées sur la Séparation Aveugle de Sources (Blind Source Separation BSS) figurent parmi les techniques cryptographiques dont l'application a connu récemment un engouement dans le domaine du cryptage de la voix et de l'image.

Cependant, de notre point de vue, les techniques de BSS sont plus adaptées à des fins de cryptanalyse plutôt qu'à des fins de cryptographie. Ceci est dû essentiellement au fait que les techniques de BSS sont, de par leur définition, des outils développés pour récupérer un ensemble de signaux de sources à partir de leurs mélanges observés sans connaître les coefficients du mélange. Il s'agit, par analogie, de la même formulation du problème de cryptanalyse à savoir la récupération d'un texte en clair (ou un ensemble de textes en clair) à partir de textes cryptés (mélanges de textes en clair et de clés cryptographiques) sans connaître les clés cryptographiques (coefficients de mélange).

Ce constat sur les limites de l'utilisation en toute sécurité, d'un point

de vue cryptographique, des techniques BSS nous a motivés pour concevoir une nouvelle technique qui pourrait contourner ces limites, ce qui a donné naissance à une technique de cryptage basée sur les sous-espaces, technique qui représente le coeur de la valeur ajoutée de cette thèse. Des tests d'évaluation de la robustesse cryptographique et de la qualité de restitution des signaux d'origines ont été conduits. Ces tests ont concerné des signaux de parole, d'image et de données.

Objectif

Dans cette thèse, nous nous sommes concentrés sur l'étude et l'analyse de l'utilisation du concept de sous-espace en étudiant en premier lieu la possibilité d'utiliser les techniques de BSS dans le domaine du cryptage. Les diverses contraintes, notamment celles inhérentes à la robustesse cryptographique, liées à l'utilisation de ces techniques sont, par la suite, analysées. Les résultats de l'analyse sont utilisés pour donner une nouvelle orientation de la recherche et du développement de techniques alternatives basés sur le concept de sous-espace.

Méthodologie

Nous procédons dans cette thèse à une analyse complète de l'utilisation des techniques BSS dans le domaine cryptographique. Notre approche est orientée "objectif" dans le sens où elle se penche sur les caractéristiques des techniques BSS qui pourraient présenter un intérêt par rapport aux exigences cryptographiques et ce, en adoptant pour des outils de crypt-analyse pour conduire cette analyse. A l'issue, de nouvelles aproches basées sur le concept de sous-espace sont conçues et proposées pour apporter des améliorations au niveau des caratéristiques de sécurité cryptographique.

Principes et rappels

Etat de la technique antérieure

Une série de différents schémas de chiffrement basés sur les techniques BSS a été proposée où les images transmises sont couvertes par une image bruit en utilisant un mélange spécifique avant le chiffrement puis elles sont récupérées par le biais de techniques BSS après le déchiffrement. Un modèle de mélange linéaire de séparation aveugle de sources a été utilisé dans le chiffrement d'image. Un algorithme de chiffrement de parole, intégrant une version modifiée du schéma de brouillage dans le domaine temporel et une méthode de brouillage d'amplitude, a été utilisé pour masquer un signal de parole avec un bruit aléatoire par la voie d'un mélange spécifique. Un schéma de chiffrement de parole utilisant les avantages du problème de séparation aveugle de sources sous-déterminée pour construire la matrice de mélange afin de chiffrer simultanément des segments multiples et augmenter le niveau de sécurité des schémas précédent, a été présenté.

Cependant, des faiblesses, d'un point de vue cryptographique, des méthodes proposées ont été relevées où il a été souligné que la sécurité contre certaines attaques de cryptanalyse n'est pas suffisamment forte notamment les attaques à texte chiffré seulement et les attaques différentielles. Aussi, la totalité des clefs générées et utilisées pour le chiffrement du signal ou de la parole doit être utilisée pour opérer le déchiffrement et récupérer le signal d'origine.

Chiffrement basé sur le sous-espace

La figure (C.1) est un schéma du bloc de chiffrement/déchiffrement basé sur les techniques sous espaces.

Le signal d'origine est divisé en L segments:

$$\mathbf{p}(t) = [p_1(t), \cdots, p_M(t)]^T, t = 1, \cdots, L \tag{C.1}$$

où M est la longuer du segment. Le signal en clair, contenant $L \times M$ échantillons, est divisé en L segments de M échantillons chacun. Les

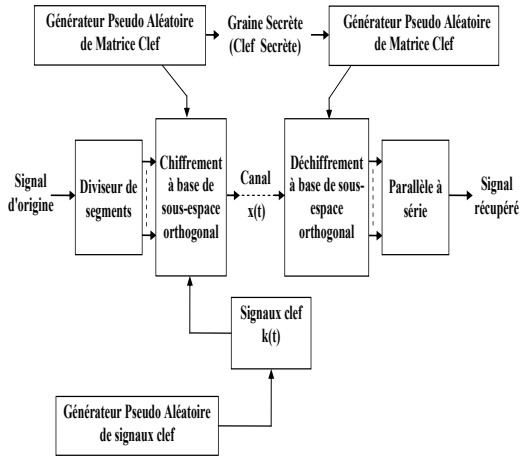


Figure C.1: Schéma block du chiffrement proposé basé sur le sous-espace orthogonal

M échantillons forment le vecteur $\mathbf{p}(t)$, de taille $M \times 1$, de l'équation (C.2). Donc, L est le nombre de segments et devient la dimension de l'échantillon du vecteur $\mathbf{x}(t)$ de l'équation (C.2). Ces segments sont utilisés dans le processus de chiffrement (le block de chiffrement basé sur le sous-espace) pour obtenir le signal chiffré suivant:

$$\mathbf{x}(t) = \mathbf{A}(t)\mathbf{p}(t) + \beta \mathbf{P}^{\perp}_{A(t)} \mathbf{B}(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{p}(t))] \qquad \text{(C.2)}$$

où $\mathbf{A}(t)$ et $\mathbf{B}(t)$ sont des $(M+1) \times M$ et $(M+1) \times M$ matrices clef à rang complet, respectivement. L'introduction des matrices $\mathbf{A}(t)$ et $\mathbf{B}(t)$ est motivée par le souhait d'agrandir l'espace clef qui serait nécessaire pour conduire une attaque de cryptanalyse. Il est à signaler que les matrices clef sont générées pour chaque vecteur $\mathbf{x}(t)$. Cette propriété rend impossible toute estimation du sous-espace du signal à partir d'un seul échantillon. Ces matrices peuvent être générées par un générateur pseudo-aléatoire avec une semence secrète qui sert de clef secrète. β est un facteur qui contrôle le rapport signal/bruit (SNR). Ce facteur (β) devrait être choisi le plus large possible pour donner un rapport

signal/bruit très petit, $\mathbf{g}(.)$ est une fonction nonlinéaire (component-wise) qui vérifie la condition suivante:

$$\mathbf{g}(0) = 0. \tag{C.3}$$

$\mathbf{k}(t)$ est un $M \times 1$ vecteur de signal clef aléatoire généré par n'importe quel générateur robuste de signaux et $\odot$ représente l'opérateur d'Hadamard. $\mathbf{P}^{\perp}_{A(t)}$ est le projecteur sur le sous-espace orthogonal à celui engendré par les colonnes de la matrice clef $\mathbf{A}(t)$ qui représente le sous-espace clef. Le projecteur $\mathbf{P}^{\perp}_{A(t)}$ est donné par:

$$\mathbf{P}^{\perp}_{A(t)} = \mathbf{I} - \mathbf{P}_{A(t)} = \mathbf{I} - \mathbf{A}(t)(\mathbf{A}(t)^H\mathbf{A}(t))^{-1}\mathbf{A}(t)^H \tag{C.4}$$

où $\mathbf{P}_{A(t)}$ est le projecteur orthogonal au sous-espace clef, et $(.)^H$ et $\mathbf{I}$ représentent l'opérateur Hermitien et la matrice identité, respectivement. Pour les besoins de l'évaluation de la robustesse, nous utilisons la fonction nonlinéaire suivante (component-wise):

$$g(v) = \frac{v}{\sqrt{1+v^2}} \tag{C.5}$$

qui vérifie la condition (C.3).

Déchiffrement

Du côté du récepteur, le vecteur de données chiffrées est projeté sur le sous-espace clef correpondant; Ceci est effectué comme suit:

$$\mathbf{x}_p(t) = \mathbf{P}_{A(t)}\mathbf{x}(t) \tag{C.6}$$

où $\mathbf{x}_p(t)$ est la donnée projetée obtenue. Du moment que les projecteurs $\mathbf{P}_{A(t)}$ et $\mathbf{P}^{\perp}_{A(t)}$ sont orthogonaux (c.à.d. $\mathbf{P}_{A(t)}\mathbf{P}^{\perp}_{A(t)} = \mathbf{0}$), la projection ci-dessus donne le résultat suivant:

$$\mathbf{x}_p(t) = \mathbf{A}(t)\mathbf{p}(t) \tag{C.7}$$

et le texte en clair d'origine (le signal déchiffré) est obtenu en utilisant la matrice clef $\mathbf{A}(t)$:

$$\mathbf{p}(t) = (\mathbf{A}(t))^{\sharp}\mathbf{x}_p(t) \tag{C.8}$$

où $(.)^{\sharp}$ représente l'opérateur pseudo-inverse.

Il est à souligner que la corrélation qui existe entre les deux termes de l'équation (C.2) va augmenter l'erreur d'estimation s'il y aurait un moyen d'estimer $\mathbf{A}$ ou son sous-espace. En plus de cette propriété, plusieurs tests ont été effectués pour mesurer la sensibilité du système proposé aux plus petites variations de matrice.

Chiffrement itératif basé sur le sous-espace orthogonal

L'approche d'itération pour un certain nombre de rounds est généralement appliquée dans les systèmes de chiffrement afin d'améliorer leurs caractéristiques de sécurité et, partant, de renforcer leur résistance aux attaques de cryptanalyse. A ce niveau, le système de chiffrement proposé basé sur le sous-espace et décrit dans la section (C) constitue un round. La sortie du premier round est réinjectée dans l'entrée pour le second round et ainsi de suite. La sortie du dernier round représente la sortie de l'ensemble du système de chiffrement itératif basé sur le sous-espace.

Chiffrement

Les segments de l'équation (C.1) sont utilisés dans le processus du chiffrement itératif basé sur le sous-espace pour obtenir le signal crypté suivant:

$$\mathbf{x}_n(t) = \mathbf{A}_n(t)\mathbf{x}_{(n-1)}(t) + \beta \mathbf{P}^{\perp}_{A_n(t)} \mathbf{B}_n(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{x}_{(n-1)}(t))]$$

où $\mathbf{x}_n(t)$ et $\mathbf{x}_{(n-1)}(t)$ représentent les $n^{ème}$ et $(n-1)^{ème}$ segments chiffré. $n \geq 1$ et $\mathbf{x}(0) = \mathbf{p}(t)$, le texte en clair. $\mathbf{A}_n(t)$ et $\mathbf{B}_n(t)$ sont $(M+1) \times M$ des matrices de rang complet, respectivement. Il est à souligner que le processus de chiffrement décrit dans (C.9) est appliqué sur différentes itérations.

Déchiffrement

Une fois le texte chiffré obtenu, la procédure de déchiffrement pourrait être réalisée en projetant le dernier segment chiffré $\mathbf{x}_{n(t)}$ tel que décrit par l'équation suivante:

$$\mathbf{x}_{p,n}(t) = \mathbf{P}_{A_n(t)}\mathbf{x}_{n(t)} \tag{C.9}$$

où $\mathbf{x}_{p,n}(t)$ est la donnée projetée obtenue. Du moment que les projecteurs $\mathbf{P}_{A_n(t)}$ et $\mathbf{P}^{\perp}_{A_n(t)}$ sont orthogonaux (c.à.d. $\mathbf{P}_{A_n(t)}\mathbf{P}^{\perp}_{A_n(t)} = \mathbf{0}$), la projection décrité ci-dessus donne le résultat suivant:

$$\mathbf{x}_{p,n}(t) = \mathbf{A}_n(t)\mathbf{x}_{(n-1)}(t) \tag{C.10}$$

Le signal déchiffré à l'itération $n-1$, est alors obtenue par:

$$\mathbf{x}_{(n-1)}(t) = (\mathbf{A}_n(t))^{\sharp}\mathbf{x}_{p,n}(t) \tag{C.11}$$

où $(.)^{\sharp}$ désigne l'opérateur pseudo-inverse. Les équations décrites ci-dessus sont appliquées de manière itérative jusqu'à restitution du texte en clair d'origine.

Chiffrement basé sur le sous-espace oblique

Dans ce chapitre, nous proposons un schéma de chiffrement basé sur le concept de sous-espace oblique plutôt que le concept orthogonal comme décrit précédemment. Les différences entre les deux approches sont présentées et une conclusion sur la valeur ajoutée de l'approche basée sur le sous-espace oblique est donnée.

Système de chiffrement basé sur le sous-espace oblique

Nous considérons que le canal de communication est idéal et que la sortie de l'étape de chiffrement est exactement l'entrée de l'étape de déchiffrement.

Chiffrement

La principale différence entre le système de chiffrement basé sur le sous-espace oblique et celui orthogonal réside dans l'opérateur de chiffrement qui est basé sur le sous-espace oblique au lieu du sous-espace orthogonal.

Le texte en clair est divisé en L segments avant d'être introduit dans l'opérateur de chiffremnt basé sur le sous-espace oblique pour produire le texte chiffré suivant (signal chiffré):

$$\mathbf{x}(t) = \mathbf{A}(t)\mathbf{p}(t) + \beta\mathbf{B}(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{p}(t))] \tag{C.12}$$

où $\mathbf{A}(t)$ et $\mathbf{B}(t)$ sont des matrices clef de rang complet de dimensions respectives $(M+1) \times M$ et $(M+1) \times 1$.

Déchiffrement

Pour effectuer le déchiffrement, le vecteur de données chiffrées reçu est projeté tel que décrit par l'équation suivante:

$$\mathbf{x}_p(t) = \mathbf{E}_{A(t)B(t)}\mathbf{x}(t) \tag{C.13}$$

où $\mathbf{x}_p(t)$ est la donnée projetée obtenue sur le sous-espace image $\langle A(t) \rangle$ obliquement au sous-espace nul $\langle B(t) \rangle$.

Sachant que:

$$\mathbf{E}_{A(t)B(t)}\mathbf{A(t)} = \mathbf{A(t)}$$

et

$$\mathbf{E}_{A(t)B(t)}\mathbf{B(t)} = 0$$

où

$$\mathbf{E}_{AB} = \mathbf{A}(\mathbf{A}^H\mathbf{P}_B^{\perp}\mathbf{A})^{-1}\mathbf{A}^H\mathbf{P}_B^{\perp}$$

et

$$\mathbf{E}_{BA} = \mathbf{P}_B(\mathbf{I} - \mathbf{E}_{AB})$$

la projection décrite ci-dessus donne le résultat suivant:

$$\mathbf{x}_p(t) = \mathbf{A}(t)\mathbf{p}(t) \tag{C.14}$$

et le texte en clair d'origine (signal déchiffré) est obtenu en utilisant la matrice clé $\mathbf{A}(t)$:

$$\mathbf{p}(t) = (\mathbf{A}(t))^{\sharp}\mathbf{x}_p(t) \tag{C.15}$$

où $(.)^{\sharp}$ désigne l'opérateur pseudo-inverse.

Chiffrement Itératif basé sur le Sous-Espace Oblique

En suivant la même méthodologie adoptée dans le chiffrement itératif basé sur le sous-espace orthogonal, le chiffrement basé sur le sous-espace oblique décrit dans la section (4.2) constitue un round dans le schéma de chiffrement itératif basé sur le sous-espace oblique. Les autres rounds sont comparables à la première et suivent la même procédure. Cela signifie que, à des fins de chiffrement, l'entrée du second round est exactement la sortie du premier round et ainsi de suite. A la fin du processus de chiffrement, disons après n rounds, la sortie du $n^{ème}$ est la sortie de l'ensemble du schéma de chiffrement itératif basé sur le sous-espace oblique.

Chiffrement

Dans le système de chiffrement iteratif basé sur le sous-espace oblique, les segments divisés décrits dans le l'équation (C.1) sont injectés dans le système pour donner le signal chiffré suivant:

$$\mathbf{x}_n(t) = \mathbf{A}_n(t)\mathbf{x}_{(n-1)}(t) + \beta\mathbf{B}_n(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{x}_{(n-1)}(t))] \tag{C.16}$$

où $\mathbf{x}_n(t)$ et $\mathbf{x}_{(n-1)}(t)$ désignent les $n^{ème}$ $(n-1)^{ème}$ segments chiffrés. $n \geq 1$ et $\mathbf{x}(0)= \mathbf{p}(t)$, le texte en clair. $\mathbf{A}_n(t)$ et $\mathbf{B}_n(t)$ sont des matrices clé de rang complet de dimensions respectives $(M+1)\times M$ et $(M+1)\times 1$. Il est à noter que le processus décrit dans l'équation (C.16) est effectué sur plusieurs itérations.

Déchiffrement

A la réception du texte chiffré, la procédure de déchiffrement peut être effectuée en projetant le dernier segment chiffré $\mathbf{x}_n(t)$ tel que décrit par

l'équation suivante:

$$\mathbf{x}_{p,n}(t) = \mathbf{E}_{A_n(t)B_n(t)}\mathbf{x}_{n(t)} \tag{C.17}$$

où $\mathbf{x}_{p,n}(t)$ est la donnée projetée obtenue sur le sous-espace image $\langle A_n(t)\rangle$ obliquement au sous-espace nul $\langle B_n(t)\rangle$.

Sachant que

$$\mathbf{E}_{A_n(t)B_n(t)}\mathbf{A}_n(t) = \mathbf{A}_n(t)$$

et

$$\mathbf{E}_{A_n(t)B_n(t)}\mathbf{B}_n(t) = 0$$

on obtient:

$$\mathbf{x}_{p,n}(t) = \mathbf{A}_n(t)\mathbf{x}_{(n-1)}(t) \tag{C.18}$$

Le signal déchiffré à l'itération $n-1$, est donné par

$$\mathbf{x}_{(n-1)}(t) = (\mathbf{A}_n(t))^\sharp \mathbf{x}_{p,n}(t) \tag{C.19}$$

où $(.)^\sharp$ désigne l'opérateur pseudo-inverse. Les équations décrites ci-dessus sont effectuées itérativement jusqu'à restitution du texte en clair d'origine.

Robustesse cryptographique des systèmes de chiffrement basés sur les sous-espaces

L'approche d'évaluation de la robustesse cryptographique est une cryptanalyse orientée vers l'application d'attaques sur les systèmes de chiffrement basés sur les sous-espaces, orthogonaux et obliques, respectivement. Les résultats de ces attaques de cryptanalyse sont utilisés pour faire une comparaison avec le schéma de chiffrement basé sur la technique BSS.

Interprétation en termes d'exigences de confusion et de diffusion

Dans la conception de la majorité des systèmes cryptographiques publiés, deux principes importants sont présents dans l'esprit du concepteur:

confusion et diffusion. La confusion est basée sur l'idée d'obscurcir la relation entre le texte en clair, le texte chiffré et les clés de chiffrement. Ceci est réalisé par le biais de mélange de linéarité et de non-linéarité.

La diffusion est l'autre principe important de la conception du système cryptographique et se fonde sur l'idée que chaque bit du texte chiffré doit dépendre de chaque bit du texte en clair et chaque bit de la clé de chiffrement. Cela garantit que les statistiques du texte en clair sont dissipées dans le texte chiffré de sorte qu'un attaquant ne peut pas prédire le texte en clair qui correspond à un texte chiffré particulier, même après avoir observé un certain nombre de textes en clair "similaires" et leurs textes chiffrés (cryptogrammes) correspondant.

En règle générale, dans la plupart des systèmes cryptographiques publiées, la substitution et la permutation sont les deux principales opérations appliquées, conjointement ou séparément, sur les textes en clair afin d'assurer la confusion et la diffusion.

Dans notre système proposé, la confusion est obtenue par la linéarité et la non-linéarité alors que l'équation (C.20) montre que l'exigence de la diffusion est assurée parce que chaque valeur du texte chiffré dépend de chaque valeur du texte en clair et de chaque valeur de la clé de chiffrement.

Attaque à texte chiffré seulement

C'est l'attaque la plus connue et la plus réaliste, car elle ne nécessite pas plus que la disponibilité des textes chiffrés.

Sensibilité à $\mathbf{P}_{A(t)}$

Si deux clés distinctes sont utilisées pour chiffrer le même texte en clair, la sensibilité d'un système cryptographique à sa clé secrète est évaluée en fonction de la différence entre les deux signaux chiffrés obtenus.

Pour plus de simplicité et de clareté, l'équation (C.2) pourrait être

reformulée comme suit:

$$\mathbf{x}(t) = \mathbf{y}_p(t) + \beta\mathbf{z}(t) \tag{C.20}$$

où $\mathbf{y}_p(t) = \mathbf{A}(t)\mathbf{p}(t)$ et $\mathbf{z}(t) = \mathbf{P}^{\perp}_{A(t)}\mathbf{B}(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{p}(t))]$. Si on considère le projecteur biaisé suivant:

$$\hat{\mathbf{P}}_{A(t)} = \mathbf{P}_{A(t)} + \epsilon\mathbf{I} \tag{C.21}$$

avec ϵ une valeur de précision finie et $\mathbf{I}$ est une matrice idéntité de taille $(M+1) \times (M+1)$. En utilisant le projecteur biaisé $\hat{\mathbf{P}}_{A(t)}$ pour le déchiffrement, on obtient:

$$\begin{aligned} \hat{\mathbf{P}}_{A(t)}\mathbf{x}(t) &= (\mathbf{P}_{A(t)} + \epsilon\mathbf{I})\mathbf{y}_p(t) + \beta(\mathbf{P}_{A(t)} + \epsilon\mathbf{I})\mathbf{z}(t) && \text{(C.22)} \\ &= (1+\epsilon)\mathbf{y}_p(t) + \beta\epsilon\mathbf{z}(t) && \text{(C.23)} \end{aligned}$$

Dans l'équation (C.23), nous avons utilisé le fait que $\mathbf{P}_{A(t)}\mathbf{y}_p(t) = \mathbf{y}_p(t)$ et $\mathbf{P}_{A(t)}\mathbf{z}(t) = 0$. Il est à noter que, d'après l'équation (C.23), les données déchiffrées en utilisant le projecteur biaisé sont toujours chiffrées suivant le système de chiffrement proposé et décrit par l'équation (C.2).

En choisissant $\beta = O(\frac{1}{\epsilon})$, l'équation (C.23) montre que, même pour de très petites valeurs de ϵ, il y a une différence significative entre les résultats obtenus en déchiffrant avec le projecteur actuel $\mathbf{P}_{A(t)}$ et sa version biaisée $\hat{\mathbf{P}}_{A(t)}$. Cela signifie que le système de chiffrement proposé basé sur le sous-espace est très sensible aux variations du projecteur. Par conséquent, il vérifie un important principe de la robustesse cryptographique à savoir la haute sensibilité aux variations des paramètres secrets. Cette grande sensibilité est vérifiée par le biais de l'expérimentation suivante:

Etape 1: Pour un projecteur et des clés générés aléatoirement $(\mathbf{P}_{A(t)}, \mathbf{k}(t))$, on obtient un texte chiffré $\mathbf{x}(t)$ correspondant à un texte en clair $\mathbf{p}(t)$.

Etape 2: Avec un projecteur biaisé $\mathbf{P}_{A(t)} + \epsilon\mathbf{I}$, on déchiffre $\mathbf{x}(t)$ pour obtenir $\hat{p}(t)$, une version estimée de $p(t)$, où ϵ dans [0,1].

Les résultats et l'analyse de cette expérimentation démontrent une grande sensibilité aux variations du projecteur.

Chiffrement itératif basé sur le sous-espace oblique Les données déchiffrées $\mathbf{x}_{(p,n)}(t)$ obtenues en appliquant le projecteur biaisé sont décrites par $\hat{\mathbf{E}}_{\mathbf{A}_n(t)\mathbf{B}_n(t)}\ \mathbf{x}_n(t)$. On obtient:

$$\begin{aligned}\hat{\mathbf{E}}_{\mathbf{A}_n(t)\mathbf{B}_n(t)}\mathbf{x}_n(t) &= (\mathbf{E}_{\mathbf{A}_n(t)\mathbf{B}_n(t)} + \epsilon\mathbf{I})\mathbf{y}_{(p,n)}(t) + \beta(\mathbf{E}_{\mathbf{A}_n(t)\mathbf{B}_n(t)} + \epsilon\mathbf{I})\mathbf{z}_n(t) \\ &= (1+\epsilon)\mathbf{y}_{(p,n)}(t) + \beta\epsilon\mathbf{z}_n(t) \qquad \text{(C.24)}\end{aligned}$$

Le résultat de l'opération de déchiffrement en utilisant un projecteur biaisé est toujours chiffré d'après le modèle de chiffrement proposé d'où la grande sensibilité du système de chiffrement itératif basé sur le sous-espace oblique.

Sensibilité aux signaux clé $\mathbf{k}(t)$

Le système de chiffremnt basé sur le sous-espace, orthogonal ou oblique, est très sensible aux signaux clé pour les mêmes raisons déjà décrites dans la sensisbilité au projecteur $\mathbf{P}_{A(t)}$. Si on considère une seconde opération de chiffrement du même texte en clair $\mathbf{p}(t)$ en utilisant la même matrice clé $\mathbf{A}(t)$. Un résultat attendu de cette opération de chiffrement devrait être le même texte chiffré $\mathbf{x}(t)$. Cependant, ce n'est pas le cas dans notre système proposé.

Ceci est dû au fait que le générateur aléatoire (ou pseudo-aléatoire) utilisé pour générer les signaux clé génére chaque fois une séquence différente. C'est une caractéristique importante qui a un impact sur la résistance du système de chiffrement proposé à l'attaque au texte chiffré seulement. L'incertitude sur le nombre de textes en clair correspondants à un nombre de texte chiffrés collectés fournit un niveau supplémentaire de résistance à cette classe d'attaque de cryptanalyse.

Sensibilité au texte en clair

Une autre propriété cryptographique requise par un système de chiffrement robuste est que le chiffrement doit être très sensible aux plus petites variations du texte en clair. Cette propriété correspond bien avec le schéma de chiffrement proposé basé sur le sous-espace, orthogonal ou oblique.

Attaque différentielle

La difficulté de résolution d'équations non linéaires peut être utile pour la conception de systèmes de chiffrement. Une attaque de différentielle est basée sur l'hypothèse que deux signaux clé identiques sont utilisés pour chiffrer au moins deux textes en clair. Cependant, l'espace clés d'un bon générateur de nombre pseudo-aléatoires, qui génère des séquences pseudo-aléatoires ayant des propriétés statistiques similaires à celles des séquences aléatoires, doit être suffisamment grand pour prévenir l'apparition de deux signaux de valeurs identiques. Par ailleurs, même si nous supposons que les deux signaux clés identiques ont été utilisés pour chiffrer les deux textes en clair, l'attaque différentielle ne peut pas être réalisée sur le système de chiffrement basé sur le sous-espace, orthogonal et oblique.

Chiffrement basé sur le sous-espace orthogonal Si on suppose que deux textes en clair $\mathbf{p}^{(1)}(t)$ et $\mathbf{p}^{(2)}(t)$ sont chiffrés en utilisant les mêmes paramètres clé $(\mathbf{P}_{A(t)}, \mathbf{k}(t))$. A partir de l'équation (C.2), on a:

$$\mathbf{x}^{(1)}(t) = \mathbf{A}(t)\mathbf{p}^{(1)}(t) + \beta\mathbf{P}^{\perp}_{A(t)}\mathbf{B}(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{p}^{(1)}(t))] \tag{C.25}$$

et

$$\mathbf{x}^{(2)}(t) = \mathbf{A}(t)\mathbf{p}^{(2)}(t) + \beta\mathbf{P}^{\perp}_{A(t)}\mathbf{B}(t)[\mathbf{k}(t) \odot \mathbf{g}(\mathbf{p}^{(2)}(t))] \tag{C.26}$$

En combinant les équations (C.25) et (C.26), on obtient:

$$\Delta_x(t) = \mathbf{A}(t)\Delta_p(t) + \beta\mathbf{P}^{\perp}_{A(t)}\mathbf{B}(t)[\mathbf{k}(t) \odot [\mathbf{g}(\mathbf{p}^{(1)}(t)) - \mathbf{g}(\mathbf{p}^{(2)}(t))]] \tag{C.27}$$

où $\Delta_x(t)$ est le différentiel de texte chiffré décrit par:

$$\Delta_x(t) = \mathbf{x}^{(1)}(t) - \mathbf{x}^{(2)}(t) \tag{C.28}$$

et $\Delta_p(t)$ est le différentiel de textes en clair décrit par:

$$\Delta_p(t) = \mathbf{p}^{(1)}(t) - \mathbf{p}^{(2)}(t) \tag{C.29}$$

Il est à noter que si la même clé est utilisée pour obtenir les textes chiffrés $\mathbf{x}^{(1)}(t)$ et $\mathbf{x}^{(2)}(t)$, le terme de la perturbation additive du sous-espace est toujours présent dans l'équation (C.27). Par ailleurs, le

différentiel de textes en clair $\Delta_p(t)$ ne peut être calculé en raison de la présence permanente des termes $\mathbf{p}^{(1)}(t)$ et $\mathbf{p}^{(2)}(t)$ dans l'équation (C.27). Ceci est dû à la corrélation existante entre le terme de la perturbation additive du sous-espace et le terme du texte en clair du système de chiffrement proposé (C.2).

Chiffrement itératif basé sur le sous-espace oblique En combinant les équations descriptives de chaque texte chiffré conformément au modèle de chiffrement itératif basé sur le sous-espace oblique et après simplification, on obtient:

$$\Delta_{\mathbf{x}_n}(t) = \mathbf{A}_n(t)\Delta_{\mathbf{x}_{(n-1)}}(t) + \beta\mathbf{B}_n(t)[\mathbf{k}(t) \odot [\mathbf{g}(\mathbf{x}^{(1)}_{(n-1)}(t)) - \mathbf{g}(\mathbf{x}^{(2)}_{(n-1)}(t))] \tag{C.30}$$

où $\Delta_{\mathbf{x}_n(t)}$ est le différentiel de textes chiffrés. Pour $n \geq 1$, le différentiel de textes chiffrés ne peut pas être calculé en raison de la présence du terme de perturbation additive du sous-espace oblique. Ceci constitue une protection contre l'attaque différentielle.

Valeur ajoutée de la fonction nonlinéaire $g(.)$

Durant le processus de conception du système de chiffremnt basé sur le sous-espace, le choix de la fonction nonlinéaire a constitué une étape cruciale. D'un côté, il fallait assurer un degré élevé de nonlinéarité et de l'autre côté, il fallait prévenir, ou du moins rendre très difficile, toute attaque de cryptanalyse connue.

Applications et évaluation des performances

Application au signal parole

Evaluation de la robustesse de sécurité

En pratique, ϵ la valeur de précision finie qui pourrait être utilisée dans une cryptanalyse par recherche exhaustive varie généralement entre 0.1 et 0.01. D'où la valeur de l'ordre de 100 choisie pour β.

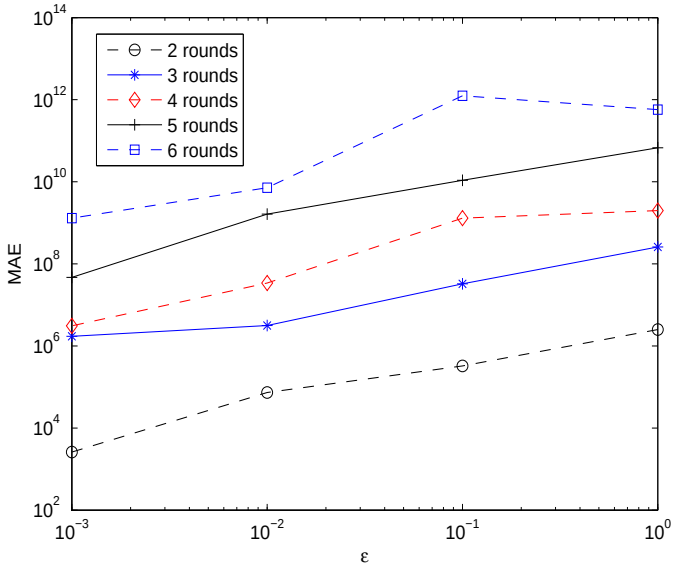
Dans les tests menés, M est choisi égale à 4, d'autres tests ont été effectués avec $M = 2$ et il n'y avait pas d'effects significatifs sur la performance de chiffrement.

Analyse de la performance en qualité

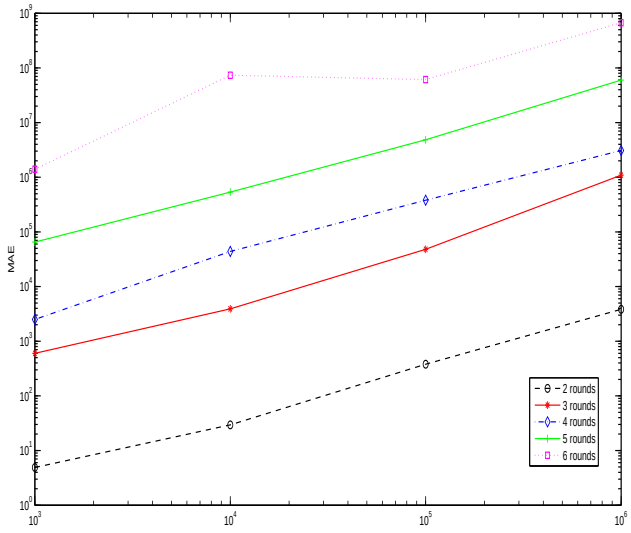
Le rapport signal-sur-bruit (SNR) en dB de chaque segment du signal chiffré et celui déchiffré est calculé. Les résultats ont été obtenus en appliquant le système de chiffrement sur un fichier de parole. Le signal d'origine a été échantillonné à une fréquence de 22.05 KHz et le nombre de bits par échantillon utilisés pour coder les données dans le fichier était 16 bits/échantillon. Les segments du signal d'origine sont bien couverts. Dans les segments décryptés, les signaux sont récupérés avec un SNR très élevé, ce qui assure une excellente qualité vocale dans le cas du chiffrement de la parole. D'autre part, les segments chiffrés présentent un très faible SNR.

Conclusion

Une nouvelle approche basée sur le concept de sous-espace est présentée dans le but de contourner les faiblesses des systèmes de chiffrement basés sur les techniques de BSS. La première approche présentée dans cette thèse est basée sur la technique du sous-espace orthogonal ensuite appliquée à la parole, l'image et des données binaires. La deuxième approche est basée sur la technique du sous-espace oblique et est également appliquée pour la parole, l'image et le cryptage des données. Pour les approches de chiffrement orthogonaux ou obliques, des versions itératives sont développées. D'une part, les itérations améliorent les performances enregistrées dans la version à un seul round et d'autre part, l'approche oblique présente des performances supérieures à celles de l'approche orthogonale. Ce travail permet d'ouvrir un nouvel axe de recherche dans les systèmes de chiffrement basés sur le concept de sous-espace.



(a)



(b)

Figure C.2: La relation expériementale, dans le chiffrement de la parole, entre l'erreur de recouvrement et la valeur de ϵ et β dans le chiffrement itératif basé sur le sous-espace oblique pour différentes itérations, (a) $\beta = 10^6$, (b) $\epsilon = 0.001$

Originalité de la contribution de la thèse

Un schéma de chiffrement basé sur le sous-espace respectivement orthogonal et oblique, à 1-round et itératif, est présenté en mettant en relief ses caractéristiques, d'un point de vue de sécurité. Tout d'abord, la matrice clef $\mathbf{A}$ est générée pour chaque segment du texte en clair, ce qui signifie qu'il y a autant de matrices clé que de segments de texte en clair. Deuxièmement, les signaux clé $\mathbf{k}(t)$ utilisés lors de l'étape de chiffrement ne sont plus nécessaires, du côté du récepteur, pour effectuer le déchiffrement. En troisième lieu, une non-linéarité est assurée dans ce système par l'utilisation d'une fonction non linéaire. En quatrième lieu, en l'absence d'un texte en clair à l'entrée du système de chiffrement proposé, il n'y a pas de sortie au niveau du côté de réception c.à.d. qu'il n'y a pas de texte chiffré. Cinquièmement, une corrélation est établie entre les différentes composantes du système de chiffrement.

De plus, la démarche itérative de chiffrement basé sur le sous-espace, à travers le processus d'application du chiffrement sur plusieurs rounds, apporte une valeur ajoutée dans le sens où elle permet l'accumulation des caratéristiques déjà garanties par le système orthogonal à un seul round. Bien sûr, l'application de plusieurs rounds dans le schéma de chiffrement itératif basé sur le sous-espace orthogonal a un coût en termes de vitesse de traitement et par conséquent en temps d'exécution. Un compromis, selon les exigences de la zone cible de l'application du schéma de chiffrement, doit être trouvé entre le nombre d'itérations et la vitesse de traitement. Cette question devient plus importante quand une implémentation matérielle est considérée.

Le système de chiffrement à base de sous-espace oblique est un schéma plus général que l'orthogonal dans le sens où ce dernier est un cas particulier de l'oblique. L'approche oblique apporte une amélioration des performances déjà enregistrées par l'approche orthogonale.

ملخص

في هذه الأطروحة، تم اقتراح نظام جديد للتعمية مستند إلى الفضاء الجزئي لتجاوز نقاط الضعف، من الناحية الأمنية، لأنظمة للتعمية التي تعتمد على تقنيات الفصل الأعمى للمصادر. لقد صممت أنظمة التعمية المستندة إلى الفضاء الجزئي المتعامد أو المنحرف، البسيطة والمتكررة، وتم تحليلها من حيث متانة الأمن وجودة الإشارات المستردة . فيما يخص تحليل الأمن، فيتم باستخدام هجمات فك التعمية في حين يتم تقييم الجودة باستخدام أدوات موضوعية و أخرى ذاتية. يتم تطبيق و تجريب نظام التعمية المقترح المستند إلى الفضاء الجزئي على الصوت والصورة والبيانات. تظهر النتائج التجريبية لنظام التعمية المقترح تحسنا ملحوظا في الأداء بالإضافة إلى بعض الميزات المهمة و المفيدة من وجهة نظر التعمية.

كلمات مفتاحية: تعمية، تشفير، فصل أعمى للمصادر، فضاء جزئي متعامد، فضاء جزئي منحرف، فك التعمية، صوت، صورة، بيانات.

Résumé

Dans cette thèse, un nouveau système de chiffrement basé sur le sous-espace est proposé pour contourner les faiblesses, d'un point de vue de sécurité, des systèmes de chiffrement basés sur les techniques de séparation aveugle de sources. Les schémas de chiffrement basés sur les sous-espaces orthogonaux ou obliques, simples et itératifs, sont conçus et analysés en termes de robustesse de sécurité et de qualité des signaux récupérés. L'analyse de la sécurité est conduite en utilisant les attaques de cryptanalyse alors que l'évaluation de la qualité est effectuée en utilisant à la fois des outils objectifs et subjectifs. Le système de chiffrement proposé basé sur le sous-espace est appliqué pour la parole, l'image et des données binaires. Les résultats expérimentaux montrent une amélioration des performances en plus de quelques fonctionnalités intéressantes et spécifiques, d'un point de vue cryptographique, apportées par le système de chiffrement proposé.

Mots clés: Chiffrement, Cryptage, Séparation aveugle de sources, Sous-espace orthogonal, Sous-espace oblique, Cryptanalyse, Parole, Image, Données binaires.

Abstract

In this thesis, a new subspace-based encryption system is proposed to bypass the weaknesses, from a security point of view, of the encryption schemes based on blind source separation techniques. Orthogonal and oblique subspace-based encryption schemes, both simple and iterative, are designed and analyzed in terms of security robustness and quality of recovered signals. Security analysis is conducted using cryptanalysis attacks whereas quality assessment is achieved using both objective and subjective tools. The proposed subspace-based encryption system is applied for speech, image and data. Experimental results show an enhancement in the performances beside some interesting and specific features, from a cryptographic point of view, brought by the proposed encryption system.

Keywords: Encryption, Enciphering, Blind source separation, Orthogonal subspace, Oblique subspace, Cryptanalysis, Speech, Image, Data.