A blind source separation based cryptography scheme for mobile military communication applications

NIKOLAOS DOUKAS, NIKOLAOS V. KARADIMAS
Department of Mathematics and Engineering Science
Hellenic Army Academy
Vari, Greece
nikolaos@doukas.net.gr, nkaradimas@sse.gr

Abstract: - Security in digital transmission is an increasingly interesting topic in a number of fields. In many cases however, the need for security is forfeited due to the high complexity of commonly used cryptosystems. The use of the underdetermined source separation problem as a basis for a cryptographic mechanism has recently been proposed. Many cryptographic algorithms, such as public key algorithms which based a common military application, use as a basis intractable number theory problems (such as integer factorization and exponentiation). Underdetermined blind source separation is also shown to have the potential to serve this purpose, as the difficulties of deriving an analytic solution to this problem have been extensively documented. This paper presents a study of blind source separation based encryption, proposes some further improvements in approaches that have already been presented and illustrates the application of the improved algorithms in the paradigm of secure speech communication. The proposed scheme is related to Independent Component Analysis Concepts. A preliminary cryptanalysis study is presented that verifies the adequacy of the new scheme for use in mobile military communication units and other applications where security is critical. The proposed scheme is also shown to be immune to some of the attacks to which existing methods were believed to be vulnerable.

Key-Words: - Blind source separation, encryption, secure digital communications.

1 Introduction

Digital data communication has become the principal means of communication on which contemporary economic, as well as social life is based [11]. Furthermore, digital data have become indispensable both for the military as well as for virtually all other security organizations [16].

1.1 Security in portable communication systems

The problem of ensuring the security of such communications, acquires therefore increasing importance. This importance is further stressed by the widespread anti-terrorist effort. This effort involves the collection and transmission of digital data and electronic information regarding activities that cover chemical, biological, nuclear and radiological agents [17]. The necessity of providing security in digital information networks has become even more acute due to the extensive use of systems that support mobility (e.g. TETRA) or Internet based systems (e.g. VOIP).

The meaning of the term security acquires a different significance depending on the application and may be perceived as a need for reliability of operation or protection of the transmitted information from tampering and interception, or combination of the above. Furthermore, depending on the needs of the organization involved, it may be necessary to protect just the useful data load or to apply additional protection to the air interface data (signaling and call information) as well. This study focuses uniquely on techniques for end-to-end encryption of the communicated information.

For speech communications, five categories of cryptographic algorithms have been proposed [9] namely frequency domain [6], [14], time domain [6], amplitude scrambling, two – dimensional, mixed scrambling methods [3], [15], as well as chaotic systems and circular transformations [17]. Encryption techniques have been proposed based on various transforms (like the fast Fourier transform, the discrete cosine transform and the wavelet transform [4]). Other approaches for robust encryption have been proposed that are based on non-linear shift registers for pseudo random number generation [21][22] (accompanied by innovative error checking – integrity checking techniques [23]). The problem of protecting data over computer networks has also been approached via adaptive encryption and quantum key distribution techniques

[24][25] as well as by utilizing the concept of virtual cryptographic devices [26].

1.2 Blind source separation revisited

Blind source separation (BSS) is a technique that has been introduced to tackle a completely different problem, namely the separation of a useful signal from within linear combinations of interfering competitors [2] and [8]. The difficulty of solving this problem, in its underdetermined version has been extensively studied [8]. The problem has been analysed to be equivalent to solving systems of equations where the numbers of unknowns is greater than the number of available equations [18]. The intractability of this problem has motivated researchers to study whether it could replace other intractable problems (e.g. integer factorization) in the construction of cryptographic algorithms [8] and [2].

The aim of this work was to design a BSS scrambler that would not produce any distortions to the data and would be of such computational complexity, so that it could be embedded in portable secure communications devices. Currently, such devices are widely used few security features [17]. This is because incorporation of such features would increase the complexity, cost and power consumption of the device, thus rendering less suitable for extensive by personnel occupied in activities needing medium or low level of security.

This paper is organized as follows: Section 2 presents BSS based speech encryption and points out where this technique is advantageous over the alternatives available. The theoretical basis supporting BSS encryption is presented and related to the field of independent component analysis. An innovative BSS based encryption scheme is presented and solutions are proposed for various practical aspects of its design. The advantages obtained from the use of the proposed technique are listed. These advantages are shown to be attained at only a small increase in the data overhead of the transmission, while the overall complexity is reduced compared to existing methods. Section 3 presents initial simulation results of the application of the proposed method for speech. The results show that, contrary to current BSS encryption schemes, the new technique does not introduce any data distortion and is hence suitable for data other than speech signals. Section 4 presents a preliminary cryptanalysis study for the new scheme and shows that it is immune to attacks to which current BSS cryptographic schemes are believed to be susceptible. Further simulation results that prove this immunity are given that focus on image data. Finally, in sections 5 and 6 conclusions resulting from this study are drawn and directions for future work are given.

2 BSS based encryption

In this section, the basics of the BSS problem, along with its underdetermined version, will be given and the way in which the BSS principles can be applied to ensure secure information transmission will be explained.

2.1 Blind Source Separation

Suppose that there exists an underlying set of M independent series of independent sequences $\underline{x}_n = \{x_{1,n}, x_{2,n}, ...x_{M,n}\}$. These series however can only be observed as a set of N linear mixtures of the above, namely: $\underline{y}_n = \{y_{1,n}, y_{2,n}, ...y_{N,n}\}$, where $\underline{y}_n = P \cdot \underline{x}_n$ with P a $M \times N$ mixing matrix. BSS aims to determine in an adaptive way a de-mixing matrix Q, such that $\underline{z}_n = P \cdot \underline{y}_n$ with $\underline{z}_n = \underline{x}_n$ [18]. Solutions to this problem and its variations have been proposed that employ various adaptive and neural network techniques [18]. Algebraic considerations can be used to prove that when N < M, the problem becomes unsolvable in the general case (unless some of the rows of P are equivalent to degenerate equations) [18]. The underdetermined case can therefore be tackled with only approximate solutions, as numerous studies have shown (e.g. [19], [18]). The same studies prove that all approximate solutions are not exact, i.e. the de-mixed information sequences are not exactly equal to the original ones.

2.2 BSS Encryption

Encryption algorithms are generally based on the impossibility of solution of intractable problems, including matrix operations [5]. BSS can be classified in this family of problems and has therefore been proposed as a basis for the development of encryption algorithms [8] and [2].

2.3 Advantages of BSS Encryption

As it has been mentioned before, conventional BSS applications, which aim at approximate solutions, employ adaptive algorithms possibly in conjunction with neural network components to converge to an approximate solution of the mixing problem they are faced with. Existing BSS encryption techniques

employ similar methods for their decryption stage (see e.g. [8] and [2]). This however is not necessary.

BSS encryption algorithms inherently require the use of some key sequences, i.e. pseudo-data sequences that will be mixed in with the useful data in a manner that will render the mixture inseparable. The keys are generated locally at both the encoder and the decoder, via the use of a pseudo random number generator. Since these keys guarantee the secrecy of the transmission, the choice of the mixing matrix becomes less relevant, provided the necessary conditions for the inseparability are met. The use of a mixing matrix, that is unknown to both ends of the information transfer and is only approximately inverted by the decryption stage, becomes redundant. It is therefore proposed that the mixing matrix also be available at the decrypting end of the information transfer. The receiver of the information can hence become significantly less computationally complex, while acquiring the ability to respond to changes in the transmitted signal statistics without any transient period or convergence delay. These advantages are not however applicable to possible cryptanalytic attackers that will still have to attempt to re-adapt (if possible) and will hence suffer from an interrupt in the data sequence. The design of the proposed modified BSS scrambler will be presented in the following section.

2.4 Independent Component Analysis

The conditions under which the underdetermined BSS problem has no analytic solution have been extensively analysed in the context of independent component analysis. The conditions for separability and inseparability, as well as for the recognition of the properties required from the mixing matrix are thoroughly explained in [1]. The definitions and theorems necessary for the foundation of the proposed scheme will be repeated here without their corresponding proof. The proof and further theoretical background for the analysis that follows can be found in bibliography [1].

- For the separation to be feasible, the information sequences must be statistically independent, i.e. their joint probability density function (pdf) must be such that:

$$f(x_1, x_2, ...x_N) = \prod_{i=1}^{N} f(x_i), \quad (1)$$

  where $f(x_i)$ is the pdf of x_i.
- There may not be more than one information sequence that follows the Gaussian distribution.
- The number of observed signals must be greater than or equal to the number of independent information signals.
- The mixing matrix must be full rank.

Consequently, if the number of sources is greater than the number of receivers, I is generally not possible to use linear operations to simultaneously recover all the information sequences. This case is referred to in bibliography as overcomplete independent component analysis or underdetermined source separation.

Definition 1: A set of m integers S = {1, 2, …, m} can be partitioned into *l,* $(l \le m)$ disjoint subsets S_i, *i =1, 2, … , l.* An $l \times m$ matrix *Z* is called a partition matrix is called a partition matrix if $z_{i,j}$ = 1 when $j \in S_i$ and $z_{i,j}$ = 0 otherwise. *Z* is called a generalized partition matrix if it is a product of an $l \times m$ partition matrix and an $m \times m$ non-singular diagonal matrix. When none of the subsets Si are empty, Z is simply a matrix in which each column has only one nonzero entry and each row has at least one nonzero entry.

Definition 2: A $k \times m$ matrix is called *l*-row decomposable if there exists an $l \times k$ matrix such that $Z = B \times R$ is an $l \times m$ generalized partition matrix.

Using the above terminology therefore, if *R* is *l*-row decomposable then there exists a matrix *B* that separates the information sequences into *l* disjoint groups, i.e. each recovered sequence $\{y_i\}$ is a linear combination of the source sequences that belong to this subgroup or:

$$y_i = \sum_{j \in S_i} z_{i,j} x_j, i = 1,2,...,l \quad (2)$$

Simple arithmetic operations lead to the conclusion that if *R* is *l*-row decomposable then *R* is also (*l*-1)-row decomposable.

The above two definitions can be used [1] to lead to the proof of the following theorems:

Theorem 1: A matrix *M* is *l*-row decomposable if and only if its columns can be grouped into *l* disjoint groups such that the column vectors in each group are linearly independent of the vectors in all the other groups.

It can consequently be proved that for $l < m$, at most *l*-1 independent information sequences can be separated out. Therefore, if a certain mixing matrix

R is not two-row decomposable, there is no linear method that can find a matrix *B* to separate the source signal into two or more disjoint groups and it is hence not possible to separate out any of the original source sequences. In order to exploit this statement, the following theorem is necessary:

Theorem 2: A $k \times m (m \geq 2k-1, m > 2)$ random with entries independent and identically chosen from some continuous distribution in the real domain matrix is not *two*-row decomposable with probability 1.

The analysis described in this section can be exploited to propose a scheme that will render the task of separating a mixture of sequences extremely difficult for an adversary that possesses no additional knowledge about these sequences, other than their mixture.

2.5 Improved BSS Scrambler design

The aims of this work was to propose a BSS scrambler design that could be incorporated in portable communication devices and render them capable of offering the same level of security compared to existing techniques such as those described in [2] and [9]. Furthermore, the design needed to be able to operate without distorting the transmitted data, a side effect that is tolerable in some cases (speech data) but not always (e.g. digital data files). Both the above aims were achieved by eliminating the convergence phase of the BSS algorithm. It will be shown that using a source matrix that is unknown to the receiver is unnecessary, given the aims that were set for the design.

The design of the improved system is depicted in Figure 1 below. In this section the overall operation of the proposed scheme is described. This operation is governed by several design parameters. Subsequent sections will describe the factors that affect the choice of these parameters, as well as a protocol for sharing of all the necessary information between the encryption and the description stages.

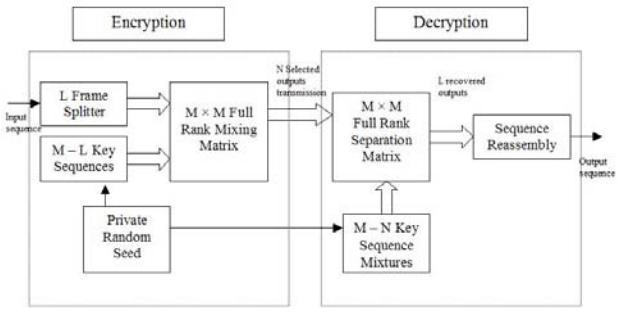

Figure 1: Proposed BSS Scrambler Block Diagram

In the encryption stage of this system the input information sequence is buffered and split into L parallel sequences, each one having a length of k samples. In Figure 1, this function is represented as the block *L-Frame splitter*. M – L key sequences are generated, using a private random seed. The statistical characteristics that these sequences need to possess will be described in a later section. The M sequences are mixed according to an M×M, full – rank, mixing matrix. N out of the M mixed signals are serialized and transmitted into the channel. In the above description L, M and N are design parameters to be determined and $L \leq N \leq M$. The choices of M and N impose certain restrictions on the structure of the mixing matrix that will be analysed later on. The frame length k is another design parameter that requires careful study for its determination. This is because k will determine the overall latency of the system, i.e. the time between the arrival of the first data item at the encryption stage and the appearance of the first data item at the output of the decryption stage. Latency can be extremely important depending on the application. In the paradigm of speech for example latency is crucial because if it exceeds a certain threshold, duplex communication between humans becomes infeasible [20]. The overall algorithmic latency of the scheme is L×k.

In the decryption stage, the observed information sequence is buffered and split into frames. These frames need to be synchronized with the corresponding frames produced during the encryption. The key sequences that were used for the encryption are re-generated locally. These sequences contain adequate information to reconstruct the M – N mixtures that were not transmitted. After this reconstruction takes place, the M available information sequences are separated using an M×M, full – rank, fixed separation matrix. This fixed separation matrix, which does not need to be estimated since the mixing matrix is known, is used in order to recover the initial information sequence frames. These are serialized and output as the recovered decrypted signal.

2.6 Distribution of key information sequences and mixing matrix

The encryption scheme proposed in this article, along with most existing algorithms of the BSS family ([2], [12]), essentially belong to the symmetric – key encryption class of algorithms. The principle impediment in the use of such algorithms is the secure sharing of the key information between

the transmitting and the receiving ends of the information flow [10], [13].

In the case of the proposed BSS encryption scheme, the key – data required to be communicated for the encoding and decoding process to get synchronized, consists of the key generator seed and the mixing matrix. The validity period of the keys is a factor that determines the level of security achieved and it is usually the case that they are frequently changed [9]. These data will be transmitted via the same encrypted channel as the useful information load of the communication.

In the context of this transfer, the random seed represents only a small overhead. The larger overhead is the transmission of the mixing matrix data. Each dimension of the mixing (or separation) matrix is equal to the frame duration. Considering that a mixing matrix is used to encrypt N frames of speech, a one-time use of the matrix would correspond to an increase of the transmission load by M^2 / N. This considerable overhead can be reduced in two ways: (a) by increasing N (the number of useful frames in the mixture) and (b) by using the same matrix for multiple frames. It should be pointed out that method (b) above does not represent a significant compromise in the overall security, since the security is maintained in the meantime by the use of the one –time information keys.

In consequence of all of the above considerations, it is proposed that the random seed be transmitted on a frame-by-frame basis, while the mixing matrix be transmitted every R frames, where R is another design parameter to be determined. Depending on the transfer rate required for the application, the overhead may be allowed to grow. This will increase the level of security to the point where the available transmission bandwidth allows.

2.7 Advantages of the improved design

The proposed technique satisfies both the aims set for it in sections 1.2 and 2.5. It offers a similar level of security as complex existing techniques such as [2] and [5] while involving a significantly lower level of computational complexity. According to [8], the act of treating the mixing matrix A as a part of the secret encryption key actually *increases* the level of security offered by the scheme. This is argued because for cryptanalysis, anything that does not belong to the key must be considered as known to adversaries.

The achievements described earlier on, are attained at the cost of an occasional overhead transmission, namely the transmission of mixing matrix data. Furthermore, the changes made to existing designs additionally eliminate transients in encrypted data separation, while the separation algorithm is converging.

Elimination of the adaptive algorithm for the separation also eliminates ambiguities in the separated information sequences recognition. This eliminates the need for the use of recognition algorithms based on heuristic criteria (like the number of zero crossings) and hence makes the scheme suitable for use in the context of any type of data and not just speech. Complexity is further reduced by virtue of the fact that there are no permutation or scale ambiguities for the separated information sequences. The second and important goal of perfect data recovery is also achieved.

Provided that the transmission of the mixing matrix data is incorporated in the encrypted transmission data, the required level of security is also attained. The complexity reduction described above, does not apply for possible eavesdroppers or other adversaries. A comprehensive study of possible cryptanalytic attacks to the scheme and its conclusions will be presented in a later section. This study is based on tests considered in bibliography virtually as standard [8].

The proposed scheme operates as an autonomous encryption module and is therefore suitable for embedding in existing digital communication systems such as TETRA or an all IP based core network

3 Application of the scheme

Initial tests of the new scheme were performed, with application to the paradigm of digital speech transmission.

3.1 Simulation results

Speech sampled at 16KHz was used and segmented into 200 ms frames. The speech was produced from a female speaker reading a continuous passage in English. The algorithm was applied on groups of 4 frames mixed with non-gaussian noise sequences. The overall transmission latency was hence less a second, a value that can be considered as acceptable for telephone-like data exchanges. In the test design, L and N were assigned the value 4, M was 8 and k was 3001 samples at 16KHz sampling rate. Non-gaussian key sequences were generated and combined with the useful data according to the 8×8 mixing matrix. According to the scheme, just 4 of the sequences where transmitted that contained useful data. With the above parameters, the

transmission efficiency is equal to 100%, since 4 frames are transmitted for each 4 frames of useful data.

In the decrypt stage, perfect synchronization was assumed to exist. The key sequences were regenerated locally and combined with the received sequences to create the full mixed sequence matrix to which the inverse transformation was applied.

The diagrams that follow show the time domain the results of the experiments on the application of the scheme.

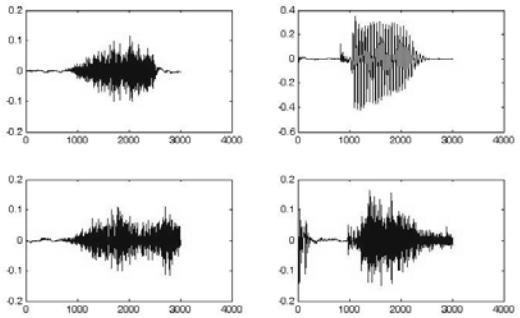

Figure 2: Samples of the original speech segments used for the tests

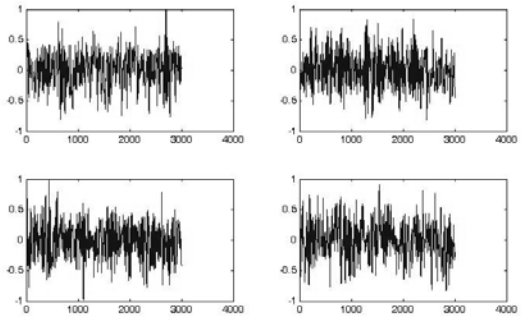

Figure 3: Sample key sequences

The objective quality measure used was signal to interference ratio (SIR). If the mixing matrix is *A* then for the mixed signal transmitted in the channel, the SIR for the *i*th frame f_i can be measured according to the formula:

$$SIR_i = \frac{A_{ii}\sum_{n=1}^{k}(f_n)^2}{\sum_{\substack{j=1 \\ j\neq i}}^{k}\sum_{m=1}^{k}\left(A_{ij}f_{jm}\right)^2} \quad (3)$$

The formula of (3) implies that the useful data mixed into the transmit signal are assumed to be additional interference. The validity of this assumption can be appreciated for the case of speech by reference to the cocktail party problem [20]. In this context, competing speech is considered to be the worst case of interference for clear speech.

Figures 2 and 3 show the clear speech data and the key sequences used for the sample experiment. From these graphs, the fact that the power level of interference is far higher than the power of the useful data sequence can be appreciated. This level difference is quantified in **Table 1**. Studies have confirmed that these levels of SIR are far lower than the ones required for the speech signal to be recognizable [20]. These findings have been confirmed in the context of this study by subjective tests. The transmitted sequences, seen in **Figure 4**, were hence confirmed to be unrecognizable as speech, a result that is consistent with the SIR figures mentioned earlier on.

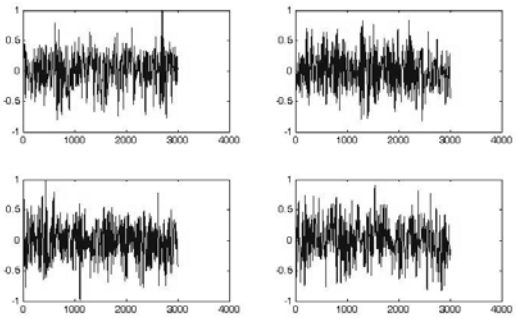

Figure 4: Sample transmitted data sequences as used for the tests

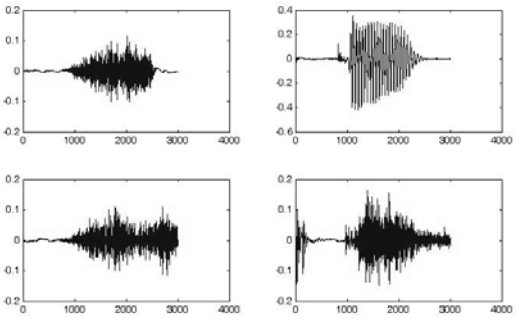

Figure 5: Sampled recovered speech data sequences

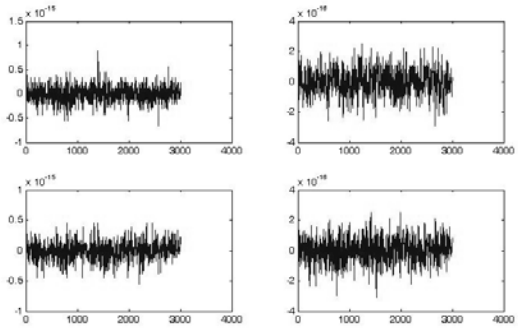

Figure 6: Error from the recovery process

In Figure 5 and Figure 6 the recovered and error sequences are shown. The recovered signal is indistinguishable from the original, while the error SIR figures shown in Table 1 support the claim that perfect sequence reconstruction is achieved.

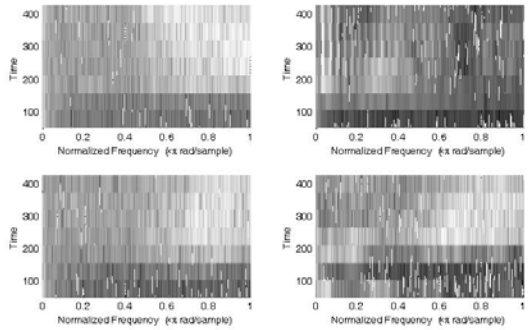

Figure 7: Original speech spectrogram

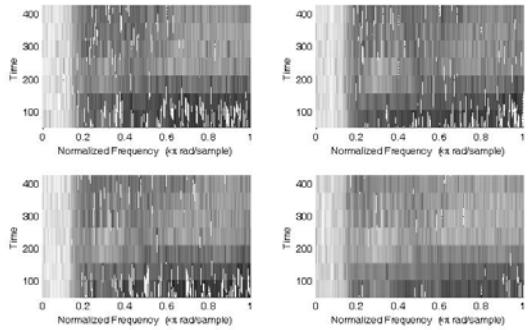

Figure 8: Encrypted speech spectrogram

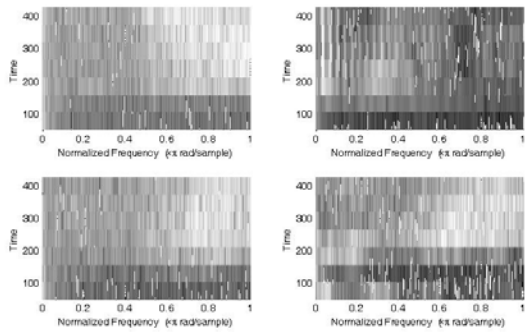

Figure 9: Recovered speech spectrogram

In Figure 7, Figure 8 and Figure 9 the spectrograms of the original, transmitted and received sequences can be inspected. The fact that the true useful sequences are completely masked can also be appreciated from these figures. In Figure 8, the spectrograms for completely different speech utterances are almost identical and this is simply due to the level of the interference present. On the contrary, the spectrogram of the recovered speech presents very little deviation from the original, a result, which is again consistent with both the objective SIR measurements presented in Table 1 and the subjective tests carried out.

Table 1: Signal to noise ratio measurements

Signal Sample	Tx SIR (dB)	Error SIR (dB)
1	-29.07	283.63
2	-12.63	302.64
3	-25.07	284.54
4	-17.07	292.60

4 Cryptanalysis of the proposed scheme

This section presents a cryptanalysis study of the new scheme using the concepts presented in [1] and presenting possible counter arguments for the objections to BSS scrambling presented in [8]. The analysis focuses on determination of the key space and consideration of the ciphertext-only attack, the differential attack, the known-plaintext attack and chosen-plaintext attack. The analysis considers some additional characteristics that affect the performance of a cryptographic system, namely its sensitivity to plaintext, to key variations and to mixing matrix variations.

The cryptanalysis carried out, takes into consideration the aims set for the proposed scheme. This scheme is meant as a means of introducing security in data communication applications that currently use no cryptographic protection or rely on encryption whose parameters are not set by the user and whose operation is controlled by unknown agents (e.g. the protection offered by the mobile telephone networks). Furthermore, the proposed scheme aims to be used for protecting messages that have a short usefulness period.

4.1 Key space calculation

A cryptosystem of the type proposed here, inevitably needs to be considered in the context of a

fixed point implementation, since it needs to protect digital data. Assuming that the mixing matrix A is an $m \times m$ matrix and that each element of A has R possible levels, then the size of the key space turns out to be $R^{2 \cdot P^2}$. Additionally, the key space is further increased due to the value of the seed used for producing the key sequences [8]. Assuming this seed has a bit size of F levels, then the overall key space can be calculated as

$$K_s = R^{2 \cdot P^2} \cdot 2^F \quad (4)$$

4.2 Ciphertext-Only attack

The entire encryption process can be formulated algebraically as

$$x[n] = A_s \cdot s[n] + A_k \cdot k[n] \quad (5)$$

with s the useful data load and k the key sequences. The decryption process can similarly be described as

$$s[n] = A_s^{-1} \cdot \left(x[n] - A_k \cdot k[n]\right) \quad (6)$$

Equation (6) can be rewritten in the form

$$\hat{s}[n] = \hat{A} x_k[n] \quad (7)$$

where

$$\hat{A} = A_s^{-1} \cdot \left(I - A_k\right) \quad (8)$$

The above results are used in [8] to claim that in order to recover $s_i[n]$, the only information necessary is $k[n]$ and the ith row of $\hat{A}$. This claim is hence used to argue that the key space calculation should be amended accordingly, yielding a much lower value than (4). The starting assumption of the argument is however not valid in the general case for the proposed scheme.

The attack needs to observe N ciphertexts that correspond to independent sequence frames or to the same sequence, in order to decrypt one. It is the case though that the proposed scheme will rarely produce either independent frames or identical frames. This conclusion can be easily deduced by considering the fact that the input sequence is segmented into time frames before transmission and the segments are mixed together with the key sequences. Additionally, for the type of communication being considered in this case, decrypting just one frame has little or no significance, since it is the continuity of the message that is of value to the communicating parties.

4.3 Differential attack

The second type of attack studied in [8] is based on observing two data sequence frames, $s_1[n]$ and $s_2[n]$ encrypted with the same key sequences. Then taking their difference, equation (5) becomes:

$$\Delta\hat{x} = \hat{A} \Delta x_s \quad (9)$$

It is hence observed that the key sequence disappears from the separation calculation and it is therefore argued that the key space calculation must be reconsidered accordingly.

There are several arguments that prevent this analysis from being applicable to the proposed BSS scrambler scheme. Firstly, it is highly unlikely that one may be able to observe two sequences encrypted with the same key or recognize that this has happened. This is so because the data is not actually encrypted with the key itself, but with key sequences that are derived from the key via a non-linear pseudo random number generation function and are used only once. Even if a cryptanalyst could know that two frames have been encrypted using the same key and managed to decrypt the data, they would still obtain just two frames of data, corresponding to two very distant time instants (depending on the periodicity of the pseudo random sequence) with very little actual value.

It is additionally argued that even the difference of two sequences could be easily recognized by human observers. Based again on the questionable assumption that the frames sharing the same key could be determined by the cryptanalyst, still the fact that one would just get two, distant in time, information snapshots, means that the usefulness of the obtained data is greatly reduced.

4.4 Known plaintext attack

This attack implies ([8]) that a malicious party obtains access to a number of plaintexts that are encrypted using the same key. Leaving aside the same key paradox, since in this case one might argue that it is valid, this prospect can be assessed as follows.

The event of a cryptanalyst obtaining access to multiple plaintexts is equivalent to the cryptanalyst being in control of the encryption device and feeding in information in an attempt to discover the decryption keys. This scenario is however once more irrelevant to the target application. The user of the device might set their personal keys and use them for communication. A third party obtaining access to this process will not manage to achieve anything significant towards obtaining access to classified information.

4.5 Chosen plaintext/ ciphertext attack

In the chosen-plaintext attack, one can freely choose a number of plaintexts and observe the corresponding ciphertexts, while in the chosen-ciphertext attack; one can freely choose a number of

ciphertexts and observe the corresponding plaintexts. So, in these attacks, one can choose plaintext differences easily, which means that the above differential known-plaintext attack still works fine in the same way [8].

The arguments against the validity of the threat of this attack are similar to the ones given in section 4.4 for the known plaintext attack. Again, the scenario to which this attack refers does not compromise the aims of the proposed scheme. If an adversary can freely observe the inputs and outputs of one system and eventually discover the keys, there is no guarantee that they will be able to decipher anything other than some expired messages.

4.6 Sensitivity to key and data

It is accepted in bibliography ([8]) as a desirable feature for encryption algorithms, that a small variation in the key, the data or the ciphertext should produce a large difference in the decoded message. As explained in [8] however, this is not the case with BSS scrambling where a small variation in any of the above sequences will result in just small errors in the speech data. In the same article it is observed though that this characteristic of BSS scrambling might be considered as a desirable feature, since it implies higher tolerance to transmission errors for encrypted data.

A further significant problem also pinpointed in [8] is the fact that the encrypted (mixed) information sequence might still be recognizable by human observers. This is due to the fact that the speech or image signals used as paradigms in this work are highly correlated and hence the encryption scheme as proposed is not suitable for masking them completely.

Leaving aside the desirability of the low sensitivity, the above problems which are significant for the performance of the scheme, may be corrected by using a simple coding scheme before encrypting the data. As a first very simple approach, a plain differential coding scheme was used on the image “Lena” and the image was then encrypted via a very simple 2×2 mixing matrix. The result was compared with the original “Lena” image, mixed in the same way. The results are shown in the following figures.

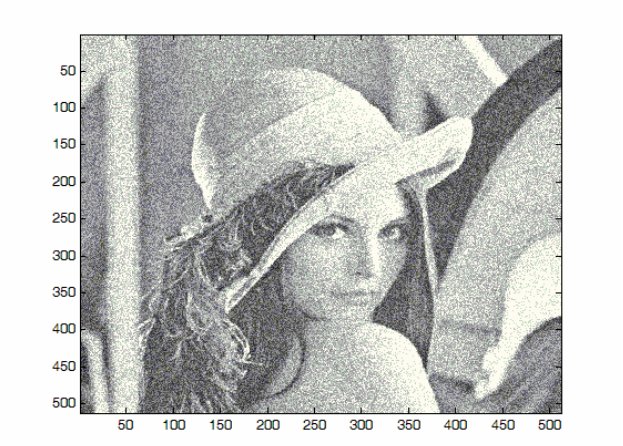

Figure 10: Original Lena image processed with a 2×2 mixing matrix

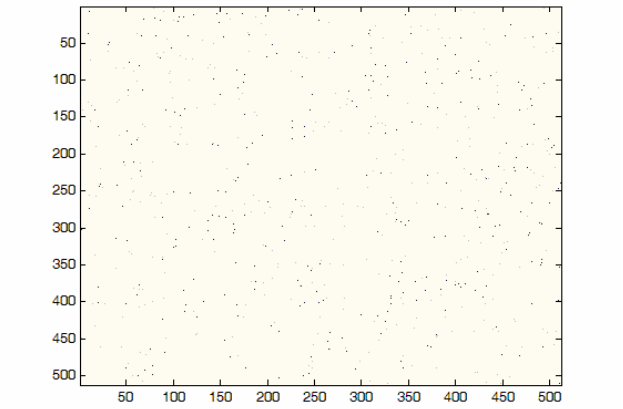

Figure 11: Differentially coded Lena image pro processed with a 2×2 mixing matrix

This example is not meant as proof of an increased level of security; it is just meant to show that preprocessing the data with a very simple coding scheme may eliminate any notion that BSS encrypted data is still recognizable by human observers.

5 Further work

The proposed scheme is being further studied with the aim of designing real-time and fixed-point versions. Both these goals involve study of further algorithmic simplifications as well as the study of issues surrounding the numeric behaviour of the algorithms and the accuracy required.

Other topics that are being investigated include automation of mixing matrix generation, key sequence statistical properties and the determination of the L, M, N and k parameters (defined in section 2.5) as a function of the required security and the tolerable levels of complexity and delay.

One more important issue under investigation is synchronization. Techniques have been proposed in

literature that may provide solutions to this problem. These are frame stealing and the fly-wheeling technique as described in [17]. These techniques offer tolerance to data distorted due to encryption, lost and out of sequence packets.

Enhancements in the domain of the level of security attained are being sought via the use of variable frame permutation within the mixing matrix. Security can be further enhanced via the exploitation of multi-user systems for incorporation of data hiding techniques [7]. This study has concluded that the weakest point of existing BSS encryption algorithms is the inherently linear nature of the operations performed on the data. Ways in which non-linear transformations, such as those presented in [26] are currently being investigated.

6 Conclusions

A novel information-scrambling scheme has been proposed, for use in portable secure communication devices has been proposed. This scheme is based on concepts from the field of Blind Source Separation and attains a level of security similar to or better than the one attained by other algorithms belonging to the BSS family of techniques at a reduced computational cost. This is achieved at the cost of a relatively small increase in the average amount of overhead data that needs to be transmitted.

The theoretical basis of the new scheme has been analysed and has been related to existing work in the domain of Independent Component Analysis.

The new scheme has been shown to be suitable for all types of data and not solely speech transmissions. Initial simulations results have been presented that confirm both the high level of security that the scheme offers and the extremely low level of distortions in the data that is recovered. It has also been shown that, with suitable selection of the schemes design parameters may reduce or even eliminate the overhead imposed by the scheme. Experiments to this respect have been carried out at 100% efficiency. A primary cryptanalytic study of the proposed scheme has been presented that showed that it is adequately secure for the applications for which it is targeted. The new scheme has also been shown to be immune to some eavesdropper attacks to which existing techniques were believed to be vulnerable.

References:

[1] Kun Liu, Hillol Kargupta, and Jessica Ryan, *Random Projection-Based Multiplicative Data Perturbation for Privacy Preserving Distributed Data Mining*, IEEE Transactions On Knowledge And Data Engineering, Vol. 18, No. 1, January 2006

[2] Qiu-Hua Lin, Fu-Liang Yin, Tie-Min Mei, and Hualou Liang, *A Blind Source Separation Based Method for Speech Encryption*, IEEE Transactions On Circuits And Systems—I: Regular Papers, Vol. 53, No. 6, June 2006.

[3] Yinian Mao and Min Wu. *A Joint Signal Processing and Cryptographic Approach to Multimedia Encryption.* IEEE Transactions On Image Processing, Vol. 15, No. 7, July 2006

[4] Kevin Sean Chan, and Faramarz Fekri. *A Block Cipher Cryptosystem Using Wavelet Transforms Over Finite Fields*. IEEE Transactions On Signal Processing, Vol. 52, No. 10, October 2004

[5] Farshid Delgosha, and Faramarz Fekri. *Public-Key Cryptography Using Paraunitary Matrices*. IEEE Transactions On Signal Processing, Vol. 54, No. 9, September 2006

[6] Marco Grangetto, Enrico Magli, and Gabriella Olmo. *Multimedia Selective Encryption by Means of Randomized Arithmetic Coding*. IEEE Transactions On Multimedia, Vol. 8, No. 5, October 2006

[7] Hafiz M. A. Malik, Rashid Ansari and Ashfaq A. Khokhar. *Robust Data Hiding in Audio Using Allpass Filters*. IEEE Transactions On Audio, Speech, And Language Processing, Vol. 15, No. 4, May 2007

[8] Shujun Li, Chengqing Li, Kwok-Tung Lo, and Guanrong Chen. *Cryptanalyzing an Encryption Scheme Based on Blind Source Separation*. IEEE Transactions On Circuits And Systems-I: Regular Papers, Vol. 55, No. 4, May 2008

[9] Jose F. de Andrade Jr, Marcello L. R. de Campos and Jose A. Apolinario Jr. *Speech Privacy For Modern Mobile Communication Systems*. Proceedings International Conference on Acoustics, Speech and Signal Processing 2008, pp 1777 – 1780.

[10] John A. MacDonald. *Cellular Authentication & Key Agreement for Service Providers*. Pervasive Computing Technologies for Healthcare, 2008. Second International Conference on Pervasive Health 2008, pp. 69 – 72

[11] Ramiro Jordan and Chaouki T. Abdallah. *Wireless Communications and Networking: An overview*. IEEE Antenna's and Propagation Magazine, Vol. 44, No. 1, February 2002

[12] Qiu-Hua Lin, Fu-Liang Yin, and Yong-Rui Zheng. *Secure Image Communication Using Blind Source Separation*. IEEE 6th CAS Symp. on Emerging Technologies: Mobile and Wireless Communications, Shanghai, China, May 31-June 2, 2004

[13] Leszek Lilien, and Bharat Bhargava. *A Scheme for Privacy-Preserving Data Dissemination*. IEEE Transactions On Systems, Man, And Cybernetics—Part A: Systems And Humans, Vol. 36, No. 3, May 2006

[14] Jooheung Lee, Narayanan Vijaykrishnan, Mary Jane Irwin and Rajarathnam Chandramouli. *Block-Based Frequency Scalable Technique for Efficient Hierarchical Coding*. IEEE Transactions On Signal Processing, Vol. 54, No. 7, July 2006

[15] Meghdad Ashtiyani, Soroor Behbahani, Saeed Asadi, Parmida Moradi Birgani. *Transmitting Encrypted Data by Wavelet Transform and Neural Network*. 2007 IEEE International Symposium on Signal Processing and Information Technology, pp. 385-389

[16] Andreas Willig. *Recent and Emerging Topics in Wireless Industrial Communications: A Selection*. IEEE Transactions On Industrial Informatics, Vol. 4, No. 2, May 2008

[17] Peter Stavroulakis. *TErrestrial Trunked RAdio – TETRA: A Global Security Tool*. Springer Verlag 2007.

[18] Andrzej Cichocki and R. Unbehauen. *Neural Networks for Optimization and Signal Processing*. Wiley, 1993

[19] Thomas Melia and Scott Rickard. *A General Framework For Extending Classic Array Processing Techniques To The Underdetermined Blind Source Separation Problem*. International Symposium on Signal Processing and Its Applications, ISSPA 2007. 9th 12-15 Feb. 2007 Page(s):1 – 4

[20] LR Rabiner, RW Schafer. *Digital Processing of Speech Signals*, PrenticeHall - Inc. Englewood Clis, New Jersey, 1978

[21] Bardis N.G, Markovskyy A.P., Andrikou D.V., "*Method for Design of pseudorandom binary sequences generators on nonlinear feedback shift register (NFSR)*", WSEAS Transactions on Communications, Issue 2, Volume 3, ISSN 1109-2742, pp: 758 - 763, April 2004.

[22] N.G.Bardis, A.Polymenopoulos, E.G.Bardis, A.P.Markovskyy, D.V.Andrikou, "*An approach to determine the complexity of random and pseudo random binary sequences*", WSEAS Transactions On Communications, Issue 1, Volume 1, ISSN 1109-2742, 2002, pp: 37 - 42.

[23] Bardis N.G, Markovskyy A.P, "*Utilization of Avalanche Transformation for Increasing of Echoplex and Checksum Data Transmission Control Reliability*", ISITA 2004 - International Symposium on Information Theory and its Applications, IEEE / SITA, Parma, Italy, October 10-13, ISBN: 4-902087-08-1, 2004.

[24] Y. Bakopoulos, N. Lygeros and A.S.Drigas. *Adaptive Encryption Protocols*. WSEAS Transactions on Communications, Issue 8, Volume 4, pp. 694-700, August 2005

[25] V.Soulioti, Y.Bakopoulos, S. Kouremenos, S.Nikolopoulos, Y.Vrettaros, A.S.Drigas. *Quantum Key Distribution and Adaptive Protocols*. WSEAS Transactions on Communications, issue 10, volume 3, p.p. 3345-3349, 2004

[26] V. Soulioti, Y. Bakopoulos, S Kouremenos, Y. Vrettaros, S. Nikolopoulos, A.S.Drigas. *Stream Ciphers created by a Discrete Dynamic System for application in the Internet*. WSEAS Transactions on Communications, Issue 2, Volume 3, April 2004.