ENCRYPTION OF MESSAGES AND IMAGES USING COMPRESSED SENSING

Marie Daňková
Doctoral Degree Programme (1), FEEC BUT
E-mail: m.dankova@phd.feec.vutbr.cz

Supervised by: Pavel Rajmic
E-mail: rajmic@feec.vutbr.cz

Abstract: The article deals with compressed sensing used to encrypt data. It allows performing signal capturing, its compression and encryption at the same time. The measurement matrix is generated using a secret key and is exploited for encryption. The article shows an example of its utilization at text and image message, moreover the Arnold transform is used in colour images for increasing security.

Keywords: compressed sensing, sparsity, cryptography, encryption, Arnold transform

1 INTRODUCTION

Conventionally, signals transmitted via a public channel are at first acquired, then compressed because of their size minimization and in the end encrypted such that an eavesdropper is not able to reveal their contents. In contrary, compressed sensing [1, 2] unites these three steps, i. e. data capturing, compression and encryption. Here, the measurement matrix is generated using a secret key. Traditional encryption algorithms (DES, AES, IDEA or RSA) are not considered as ideal for encryption of images, mainly due to big redundant blocks in images. Therefore utilization of this approach in this area is perspective [3].

Usefulness of compressed sensing cryptography is demonstrated on text messages and colour image messages. The possibility of increasing security of image cryptogram by using Arnold transform is there also shortly mentioned.

The article is structured as follows: basic scheme of compressed sensing is stated in section 2. Section 3 describes scheme of encryption and decryption using compressed sensing. This scheme is demonstrated on several examples in section 4 .

2 COMPRESSED SENSING

Compressed sensing (compressive sampling, CS) captures signal linearly and non-adaptively only as many times as really needed. Compressed sensing is applicable due to sparsity of the measured signal (or due to some other a priori information about it).

2.1 SPARSE REPRESENTATION OF SIGNALS

Signal $\mathbf{y} \in \mathbb{R}^m$ can be represented as linear combination of basic "building blocks" $\mathbf{a}_i$:

$$\mathbf{y} = \sum_i x_i \mathbf{a}_i = \mathbf{A}\mathbf{x}, \tag{1}$$

where matrix $\mathbf{A} = [\mathbf{a}_1, \dots, \mathbf{a}_n] \in \mathbb{R}^{m \times n}$, $m < n$, $\mathbf{x} \in \mathbb{R}^n$ is a vector of weight. We assume that matrix $\mathbf{A}$ has full rank and therefore infinitely many solutions to problem (1) exist. Only sparse solutions are of our interest, i. e. solutions with as many zero components in **x** as possible. Vector **x** is *k-sparse* if holds: $\|\mathbf{x}\|_0 \leq k$, where $\|\cdot\|_0$ is ℓ_0-norm which is simply the number of non-zero elements. Thus a k-sparse vector has as most k non-zero components. Relative sparsity is $\frac{\|\mathbf{x}\|_0}{n}$, where n is length of vector **x**.

Sparse solutions can be found using this minimization problem:

$$\min_{\mathbf{x}} \|\mathbf{x}\|_0 \text{ subject to } \mathbf{A}\mathbf{x} = \mathbf{y}. \tag{P0}$$

Optimization problem (P0) is usually relaxed (to be convex) and therefore computationally plausible:

$$\min_{\mathbf{x}} \|\mathbf{x}\|_1 \text{ subject to } \mathbf{A}\mathbf{x} = \mathbf{y}, \tag{P1}$$

where $\|\mathbf{x}\|_1 = \sum_{i=1}^{n} |x_i|$ is ℓ_1-norm of vector **x**. Also some tolerance ε from exact solution is usually allowed, i. e. using $\|\mathbf{A}\mathbf{x} - \mathbf{y}\| < \varepsilon$ instead of equality $\mathbf{A}\mathbf{x} = \mathbf{y}$ [4, 5].

Problem (P0) can be heuristically approximated using so called greedy algorithms such as OMP (Orthogonal Matching Pursuit) or MP (Matching Pursuit) [6]; problem (P1) can be solved by linear programming or using the so called proximal iterative methods [7].

2.2 Compressed sensing

Compressed sensing solves the same problem as (P0) but matrix **A** has a special design. Let Ψ be a basis in $\mathbb{R}^n$. Suppose that signal **z** has k-sparse representation **x** in this basis $\mathbf{z} = \Psi\mathbf{x}$. The goal of CS is taking only “small amount” of non-adaptive measurements (scalars products with the signal), mathematically $\mathbf{y} = \mathbf{P}\mathbf{z} = \mathbf{P}\Psi\mathbf{x}$. Here, **P** is so called measurement matrix $m \times n$ and components of vector **y** are results of measurement, i. e. linear combinations of signal samples. The number of measurement is $m \ll n$. In CS, matrix $\mathbf{A} = \mathbf{P}\Psi$; in summary we have this problem:

$$\min_{\mathbf{x}} \|\mathbf{x}\|_0 \text{ subject to } \mathbf{y} = \mathbf{P}\Psi\mathbf{x}. \tag{P0$'$}$$

Measurement matrices are usually considered as $\mathbf{P} = \mathbf{R}\Phi$. Here, Φ is matrix $n \times n$ (often random) and **R** is matrix formed from identity matrix $n \times n$ keeping only some (randomly) selected rows so it has the function of selection rows from Φ. So in summary matrix $\mathbf{A} = \mathbf{R}\Phi\Psi$.

The number of measurement needed to successfully reconstruct the signal (i. e. number of rows m of matrix **P**) depends on the mutual coherence μ:

$$\mu([\Phi, \Psi]) = \max_{1 \leq i,j \leq n} \left| \Psi_i^\top \Phi_j \right|.$$

The higher mutual coherence is, the more measurements m are needed. Therefore, one usually looks for pairs Ψ, Φ with as low coherence as possible [1, 2, 5].

3 ENCRYPTION AND DECRYPTION USING COMPRESSED SENSING

Usually, real signals are first sampled and then compressed to minimize their size. Further, this data are encrypted using secret key and sent by public channel to the receiver. The receiver is able to decrypt the data because he also knows the key.

In contrary, compressed sensing exploits all this operations – i. e. sampling, compression and encryption – at the same time. Here, secret key is used to generate the measurement matrix **P** for compressed sensing. Data are also transmitted via a public channel to the receiver that can reconstruct them because he knows the secret key.

Let assume that Alice wants to send a secret message $\mathbf{x} \in \mathbb{R}^n$ to Bob. If the message is not sufficiently sparse, Alice uses some suitable basis Ψ to “sparsify” its representation. Alice chooses randomly some key i (all keys from whole key space have the same probability of selection). With this key, she generates pseudo-random Gaussian measurement matrix $\mathbf{P}_i$ (secret key serves as a seed for Gaussian pseudo-random number generator; using this generator, a sequence of pseudo-random numbers is generated and this sequence forms the columns of the measurement matrix). She encrypts the message to the cryptogram $\mathbf{y} = \mathbf{P}_i\mathbf{x}$. Alice sends the cryptogram to Bob who also know the key and he is able to decrypt the message by solving the problem (P0′) or its relaxed version (P1) (it is appropriate to Alice verify herself by decrypting if proposed matrix enables proper reconstruction because all possible matrices $\mathbf{P}_i$ don’t have to satisfy conditions needed for finding original $\mathbf{x}$; sizes of measurement matrix are given experimentally for certain category of signals) [8].

If the encrypted message is too long, it is divided to smaller blocks which are encrypted separately. In case of colour images, it is possible to encrypt each of RBG channel separately using different keys to increase the secrecy. Article [3] proposes “mixing up” the encrypted pixels (i. e. after CS) using Arnold transform to additional increasing the secrecy. Let $(x,y)^\top$ be pixel coordinate of square image size $N \times N$. Then discrete Arnold transform maps the point $(x,y)^\top$ to another integer point $(x',y')^\top$:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod} N),$$

where $x,y \in \{0,1,\dots,N-1\}$. This transform is applied iteratively to the image; the number of iterations is another secret parameter in encryption.

The cryptosystem does not provide perfect secrecy as is shown e. g. in [8] and [9]. Bruce force attack is possible to the compressed sensing based cryptosystem or more sophisticate attack is possible using symmetry and sparsity structure of compressed sensing [10]. It is also impossible to learn a secret key from the plaintext-ciphertext pair, only the measurement matrix can be derived from sufficient number of this pairs using the same key and not using Arnold transform. Therefore it is better to change a key often. Unlike traditional cryptosystems, modes of operations used for block chaining can not be used in this type of cryptosystems because cryptogram has not the same length as plaintext and moreover if we add ciphertext to the plaintext (to its first vector elements) the assumption of the sparsity should be violated.

4 EXPERIMENTAL RESULTS

This part shows several simple examples of possible using compressed sensing based cryptography. Algorithm OMP was used to reconstruction original massage/image in all given examples.

4.1 TEXT MESSAGE

For encryption the text message, we assign number 1–26 to the letters A–Z, 0 to the space between words. We express the numbers as five-digit binary numbers. The sequence of binary-digit code forms sparse vector so we are able to encrypt it using compressed sensing.

Example: Alice wants to send a message to Bob:

TOTO JE TAJNY VZKAZ PRO BOBA

(*Remark: The message is in Czech with the meaning “This is a secret message for Bob”.*) We assign the binary digit numbers to each character in the message:

T	O	T	O		J	E		T	A	J
10100	01111	10100	01111	00000	01010	00101	00000	10100	00001	01010

N	Y		V	Z	K	A	Z		P	R
01110	11001	00000	10110	11010	01011	00001	11010	00000	10000	10010

O		B	O	B	A
01111	00000	00010	01111	00010	00001

The binary code forms a vector of length 140; 54 vector elements are non-zero so this vector has relative sparsity 0.3857. It was checked experimentally that measurement matrix (generated with secret key) must have at least compression ratio 0.8 (i. e. matrix size 112×140) for successful reconstruction of message.

4.2 Colour image

Common images are not sparse and it is needed to utilize some suitable representation basis for using CS. For the purpose of demonstration of CS encryption of colour image, the image shown in Fig. 1(a) has been used. The discrete cosine transform was used as the sparsifying basis Ψ. This image has been divided into blocks 8×8 px in which CS was applied to each RBG channel separately. Reconstruction from 75 % of measurements isn't exact but with small relative error 0.1812 (see Fig. 1(b)).

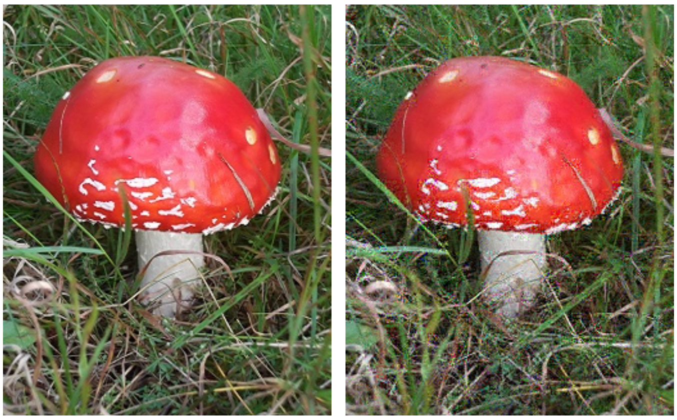
Arnold transform can be used in each block (on each RGB channel separately) after the CS. For illustration, Arnold transform of a square image (Fig. 2(a)) is shown on Fig. 2(b)–2(f) after different number of iterations (equal for each RGB channel).

5 CONCLUSION

The article presents a possibility of using compressed sensing as cryptosystem. Measurement matrix (in CS) is generated according to the secret key and it is used also for encryption. Demonstrations were presented at text and image message. In addition, application of Arnold transform was shown on colour image to increase cryptogram secrecy.

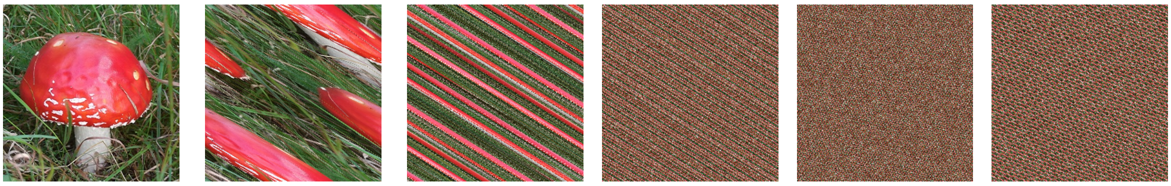
ACKNOWLEDGEMENT

The research was supported by the SIX project registration number CZ.1.05/2.1.00/03.0072.



(a) (b)

Figure 1: (a) Original image and (b) decrypted.



(a) original image (b) 1 iteration (c) 3 iterations (d) 5 iterations (e) 10 iterations (f) 13 iterations

Figure 2: Arnold transform of image toadstool (a) after different number of iterations (b)–(f).

REFERENCES

[1] Candès, E. J.; Wakin, M. B.: An introduction to compressive sampling. Signal Processing Magazine, IEEE, vol.25, no.2, pp.21,30, March 2008, doi: 10.1109/MSP.2007.914731.

[2] Hrbáček, R.; Rajmic, P.; Veselý, V.; Špiřík, J.: Sparse Representation of Signals: Compressed Sensing (in Czech). *Elektrorevue*, 2011, vol. 2011, n. 67, p. 1–8. ISSN: 1213- 1539. URL: `http://elektrorevue.cz/cz/download/ridke-reprezentace-signalu--komprimovane-snimani/`

[3] Sreedhanya, A. V.; Soman, K. P.: Secrecy of Cryptography with Compressed Sensing. 2012 International Conference on Advances in Computing and Communications. IEEE, 2012, p. 207-210. DOI: 10.1109/ICACC.2012.48.

[4] Hrbáček, R.; Rajmic, P.; Veselý, V.; Špiřík, J.: Sparse Representation of Signals: An Introduction (in Czech). *Elektrorevue*, 2011, vol. 2011, n. 50, p. 1–10. ISSN: 1213- 1539. URL: `www.elektrorevue.cz/files/200000751-638ac6484b`

[5] Daňková, M.: Compressed Sensing in Magnetic Resonance Perfusion Imaging (in Czech). Brno University of Technology, Faculty of Mechanical Engineering, 2014. 56 p. Supervisor: Mgr. Pavel Rajmic, Ph.D.

[6] Elad, M.: Sparse and Redundant Representations: From Theory to Applications in Signal and Image Processing. New York: Springer, 2010, 376 p. ISBN 978-1-4419-7010-7.

[7] Combettes, P. L.; Pesquet, J.-C.: Proximal Splitting Methods in Signal Processing. *Fixed-Point Algorithms for Inverse Problems in Science and Engineering*. Springer, 2011.

[8] Rachlin, Y.; Barun, D.: The Secrecy of Compressed Sensing Measurements. 2008 46th Annual Allerton Conference on Communication, Control, and Computing. 2008. DOI: 10.1109/allerton.2008.4797641.

[9] Mayiami, M. R.; Seyfe, B.; Bafghi; H. G.: Perfect Secrecy via Compressed Sensing. Communication and Information Theory (IWCIT), 2013 Iran Workshop on , vol., no., pp.1,5, 8-9 May 2013. doi: 10.1109/IWCIT.2013.6555751

[10] Orsdemir, A.; Altun, H. O.; Sharma, G.; Bocko, M. F.: On the Security and Robustness of Encryption via Compressed Sensing. MILCOM 2008 - 2008 IEEE Military Communications Conference. 2008. DOI: 10.1109/milcom.2008.4753187.