NOTES TO AUTHORS

The following types of articles will be published:

- full-length articles describing original research;
- short articles, also reporting original work, but shorter and more concise as regards the subject matter; there should be no difference in the quality of research described in either type of article;
- reviews, which should be a critical evaluation of the current stage of research on a particular facet of environmental problems;
- invited, accelerated articles, stimulating the up-to-data research;
- matter for discussion, concerning the current news.

Every article will be reviewed. The Editorial Board of the "Polish Journal of Environmental Studies", assisted by referees, will screen the submitted articles. Papers accepted for publication must not have been published elsewhere. Authors of papers concerning the experiments with animals are requested to include the opinion and approval of Local Commitee of Ethics.

Manuscripts

Papers should be typewritten on one side of a page (1.5 -spaced, font size 12, a margin of 2.5cm on all four sides of the paper). Two copies of a text, in English and a WORD (RTF) file on the diskette, should be sent to the editor. Authors are advised to keep a copy for themselves.

Proofs

The address to which proofs are to be sent should accompany the paper. Proofs should be carefuly checked and returned immediately.

The recommended order of presentation

- T i t l e
- A b s t r a c t. An abstract of about 100 words, stating the features and drawing attention to the novel aspects.
- K e y w o r d s. Up to 5 keywords or keyphrases, indicating the topic of importance in the work.
- I n t r o d u c t i o n. An introductory statement of the subject under investigation with any essential historical background.
- E x p e r i m e n t a l p r o c e d u r e s. Working details must be given concisely; well-known operations should not be described in detail.
- R e s u l t s. These could be presented in tabular or graph form, with appropriate statistical evaluation.
- D i s c u s s i o n of r e s u l t s. Statement of conclusions drawn from the work.

- U n i t s a n d n o m e n c l a t u r e. The SI system of units and current internationally recognised (IUPAC) chemical nomenclature should be used. Common trivial names may be used, but should first be defined in terms of IUPAC nomenclature.
- I l l u s t r a t i o n s for reproduction should be clearly drawn on separate sheets of paper and submitted in duplicate.
- R e f e r e n c e s should be indicated in the text by consecutive numbers and the full references should be listed in the same order at the end of the article in the following form:

  REFERENCES

  1. FILLERY J. R. P. Studies on denitrification. Soil Sx. Am. J. **43** (6), 1124, **1979**.
  2. ALBERTS B., BRAY D., LEWIS J., RAFF M., ROBERTS K., WATSON J. Molecular Biology of the Cell, 2nd ed.; Garland Publishing: New York, pp 300-323, **1989**.
  3. SHARMA M. C., SHAPIRO B. H. purification and characterization of constituent testosteron 2 a-hydroxylaze (cytochrome P450a) from mouse liver. Archiv. Biochem. Biophys. **316**, 478, **1995**.

SOME EXAMPLE OF THE PAPER (PATTERN)

dr inż. Mariusz Borawski
Szczecin University of Technology
Faculty of Computer Science and Information Technology
e-maol: mborawski@wi.ps.pl

Generalized Transformation Form

Abstract

Paper presents application of generalized transformation form for information encryption. It allows encryption of multiple information with different keys in one data sequence, and its decoding depends on access to key. Fact that two keys can be used to decode the same information, one key can be the public key and the other private key

Keywords: transformation forms, cryptography, encryption and decryption algorithm

Introduction

Transforms play a crucial role in various branches of science. In image processing, its 2D forms are used for filtration, selection of features for recognition, etc[1]. There is a multitude of various 2D transforms[2]: e.g. Fourier, cosine, wavelet, Hadamard.

[1] J. S. Lim: Two-dimensional signal and image processing – Englewood Clifs, Prentice-Hall International Inc., 1990

[2] A. K. Jain: Fundamentals of Digital Image Processing – Englewood Clifs, Prentice-Hall International Inc., 1989

Transforms can be introduced in different ways. For discrete transforms used in image processing, one possibility is open by vector calculus. In vector calculus transforms can be treated as transformations of the coordinate system. Transformation of coordinate system changes components of all vectors, related to this system. In this interpretation, transform can be viewed as "algorithm" for calculation of "new" coordinates based on "old" ones.

In tensor calculus it is possible to express such transformation of coordinates without reference to specific coordinate system – in form that could be called general form of transformation. Paper presents this general form of transformation, method on deriving its parameters and some practical applications.

Transformation of coordinates

Given is the set of linearly independent vectors, forming affine coordinate system $\underset{1}{e},\underset{2}{e},\ldots,\underset{n}{e}$. Coordinates of any vector x relative to this coordinate system can be expressed as[3]:

$$x = x^1 \underset{1}{e} + x^2 \underset{2}{e} + \ldots + x^n \underset{n}{e}. \tag{1}$$

In conformance with conventions used in tensor calculus, subscripts designate the consecutive vector's numbers, right subscripts – coordinates of covariant vectors, and right superscripts – coordinates of contravariant vectors.

Coordinate system $\underset{1}{e},\underset{2}{e},\ldots,\underset{n}{e}$ can be transformed into new coordinate system $\underset{1'}{e'},\underset{2'}{e'},\ldots,\underset{n'}{e'}$. Dependencies between "old" and "new" coordinate system can be written as[4]:

$$\begin{cases} \underset{1'}{e'} = A^1_{1'} \underset{1}{e} + A^2_{1'} \underset{2}{e} + \ldots + A^n_{1'} \underset{n}{e} \\ \underset{2'}{e'} = A^1_{2'} \underset{1}{e} + A^2_{2'} \underset{2}{e} + \ldots + A^n_{2'} \underset{n}{e} \\ \vdots \\ \underset{n'}{e'} = A^1_{n'} \underset{1}{e} + A^2_{n'} \underset{2}{e} + \ldots + A^n_{n'} \underset{n}{e} \end{cases}. \tag{2}$$

Matrix $A^j_{i'}$ denotes the transformation matrix of coordinate system $\underset{1}{e},\underset{2}{e},\ldots,\underset{n}{e}$ into coordinate system $\underset{1'}{e'},\underset{2'}{e'},\ldots,\underset{n'}{e'}$. For any transformation matrix of coordinate system $A^j_{i'}$ there is such transformation matrix of coordinates $A^{i'}_j$, that we have[5]:

---

[3] P. K. Raszewskij: Rimanowa geometrija i tenzornyj analiz – Moskwa, Nauka, 1964

[4] P. K. Raszewskij: *op. cit.* pp 11

[5] E. Karaśkiewicz: Zarys teorii wektorów i tensorów – Warszawa, PWN, 1974

$$A_{i'}^{j} A_{j}^{i'} = \delta_{i}^{j} . \tag{3}$$

This matrix allows to calculate coordinates of the vector in respect to coordinate system $\mathop{e}_{1}, \mathop{e}_{2}, \ldots, \mathop{e}_{n}$, based on its coordinates in respect to system $\mathop{e'}_{1'}, \mathop{e'}_{2'}, \ldots, \mathop{e'}_{n'}$[6]:

$$x^{i'} = A_{i}^{i'} x^{i} . \tag{4}$$

Expression (4) is generalized form of discrete transformation. Filling in the matrix of coordinate transformation $A_{j}^{i'}$ with relevant values, we can obtain any discrete transformation.

Forming the transformation matrix based on given basis functions

For given basis vectors, i.e. basis functions, we can determine the transformation matrix $A_{j}^{i'}$ finding its entries. For example, let's check the relation of generalized form of transformation, with discrete 1D cosine transform, given by the formula[7]:

$$S_{DCT}(k) = \alpha(k) \sum_{n=0}^{N-1} s(n) \cos\left[\frac{\pi(2n+1)k}{2N} \right], \tag{5}$$

where $n = 0,1,\ldots,N-1$, N is a number of samples of analyzed signal, and $\alpha(k)$ equals to:

$$\alpha(k) = \begin{cases} \sqrt{\dfrac{1}{N}} & \text{dla} \quad k = 0 \\ \sqrt{\dfrac{2}{N}} & \text{dla} \quad 1 \le k \le N-1 \end{cases} . \tag{6}$$

Taking that N is a dimension of the space, formula (5) can be expressed as:

$$x^{i'} = \begin{cases} \sum_{i=1}^{N} \sqrt{\dfrac{1}{N}} \cos\left[\dfrac{\pi(2i-1)(i'-1)}{2N} \right] x^{i} & \text{dla} \quad i' = 1 \\ \sum_{i=1}^{N} \sqrt{\dfrac{2}{N}} \cos\left[\dfrac{\pi(2i-1)(i'-1)}{2N} \right] x^{i} & \text{dla} \quad 1 \le i' \le N \end{cases} , \tag{7}$$

hence:

$$A_{i}^{i'} = \begin{cases} \sqrt{\dfrac{1}{N}} \cos\left[\dfrac{\pi(2i-1)(i'-1)}{2N} \right] & \text{dla} \quad i' = 1 \\ \sqrt{\dfrac{2}{N}} \cos\left[\dfrac{\pi(2i-1)(i'-1)}{2N} \right] & \text{dla} \quad 1 \le i' \le N \end{cases} . \tag{8}$$

We can see, that the entries of the transformation matrix $A_{j}^{i'}$ contain the tabulated basis functions of cosine transform.

By analogy, we can tabulate the Discrete Fourier Transform, given by the formula[8]:

---

[6] E. Karaśkiewicz: *op. cit* .

[7] H. Schroeder: One- and Multidimensional Signal Processing – Chichester, John Wiley and Sons, LTD, 2000

$$S_{DFT}(k) = \frac{1}{N}\sum_{n=0}^{N-1} s(n)\exp\left[\sqrt{-1}\left(\frac{2\pi}{N}\right)kn\right], \tag{9}$$

and, in this case the formula (8) will have the form:

$$A_i^{i'} = \frac{1}{N}\exp\left[\sqrt{-1}\left(\frac{2\pi}{N}\right)(i-1)(i'-1)\right]. \tag{10}$$

Similarly, tabulating the basis function of discrete transforms, we can express them in the form given by the formula (4). As the basis functions, we can use any set of functions $f_i(x)$:

$$A_i^{i'} = f_{i'}(i), \tag{11}$$

under the condition, that the transformation matrix $A_i^{i'}$ will have the inverse matrix $A_{i'}^{i}$, i.e. determinant $\det\left(A_i^{i'}\right)$ is not vanishing. Subject to $\det\left(A_i^{i'}\right) = 0$, set of basis function is a linearly dependent set. Practically, we could also use such a set, but we have to remember that it will be impossible to recover the original data after its transformation in such a system. An example of such a system is the following set of basis functions:

$$f_{i'}(k) = \begin{cases} \dfrac{x(2k) + x(2k+1)}{2} & \text{dla} \quad k = i' \\ 0 & \text{dla} \quad k \neq i' \end{cases}, \tag{12}$$

for which the transformation matrix has the form:

$$A_i^{i'} = \begin{cases} \dfrac{x(2i-2) + x(2i-1)}{2} & \text{dla} \quad i = i' \\ 0 & \text{dla} \quad i \neq i' \end{cases}. \tag{13}$$

Discrete form of such transformation will result in splitting the signal into two parts. First part contains whole signal with reduced number of data caused by averaging, and second part consisting of sequence of zeros. In this case the exact recovering the original signal is not possible.

Finding the transformation matrix for unknown basis functions

Any transformation of vector coordinates in case of coordinate system given by n – vectors into another n - vectors coordinate system, is described by n simultaneous equations with n - coefficients. It gives us $n \times n$ unknowns contained in the matrix $A_j^{i'}$. In order to find the matrix $A_j^{i'}$, we must have n vectors with known coordinates in „old" and „new" frames of coordinates. This will form n sets of equations, each set consisting of n equations:

---

[8] A. Oppenheim, R. Schafer, J. Buck: Discrete-Time Signal Processing – International Edition 2nd Edition, 1999

$$
\begin{cases}
x'^{1'}_{1'} = A^{1'}_{1}\,x^{1}_{1} + A^{1'}_{2}\,x^{2}_{1} + \ldots + A^{1'}_{n}\,x^{n}_{1} \\
x'^{1'}_{2'} = A^{1'}_{1}\,x^{1}_{2} + A^{1'}_{2}\,x^{2}_{2} + \ldots + A^{1'}_{n}\,x^{n}_{2} \\
\vdots \\
x'^{1'}_{n'} = A^{1'}_{1}\,x^{1}_{n} + A^{1'}_{2}\,x^{2}_{n} + \ldots + A^{1'}_{n}\,x^{n}_{n}
\end{cases}
\begin{cases}
x'^{2'}_{1'} = A^{2'}_{1}\,x^{1}_{1} + A^{2'}_{2}\,x^{2}_{1} + \ldots + A^{2'}_{n}\,x^{n}_{1} \\
x'^{2'}_{2'} = A^{2'}_{1}\,x^{1}_{2} + A^{2'}_{2}\,x^{2}_{2} + \ldots + A^{2'}_{n}\,x^{n}_{2} \\
\vdots \\
x'^{2'}_{n'} = A^{2'}_{1}\,x^{1}_{n} + A^{2'}_{2}\,x^{2}_{n} + \ldots + A^{2'}_{n}\,x^{n}_{n}
\end{cases}
\begin{cases}
x'^{n'}_{1'} = A^{n'}_{1}\,x^{1}_{1} + A^{n'}_{2}\,x^{2}_{1} + \ldots + A^{n'}_{n}\,x^{n}_{1} \\
x'^{n'}_{2'} = A^{n'}_{1}\,x^{1}_{2} + A^{n'}_{2}\,x^{2}_{2} + \ldots + A^{n'}_{n}\,x^{n}_{2} \\
\vdots \\
x'^{n'}_{n'} = A^{n'}_{1}\,x^{1}_{n} + A^{n'}_{2}\,x^{2}_{n} + \ldots + A^{n'}_{n}\,x^{n}_{n}
\end{cases}
\qquad (14)
$$

Application of generalized transformation in cryptography

The transformation matrix $A^{i'}_{j}$ allows to transform one data set into any other data set, under the condition of equal cardinality of both sets. Let consider example of twenty three elements data sequence:

$$
\begin{aligned}
x^{i} &= \text{'}Alice\ has\ cat\text{'} \\
x^{i'} &= \text{'}Cat\ has\ Alice\text{'}
\end{aligned}
\qquad (15)
$$

Data sequence x^{i} is an input sequence, and $x^{i'}$ is an output sequence. In order to determine the transformation matrix, we must have another twenty three input and output sequences. Lacking sequences could be generated randomly. This will give us transformation, converting the sequence „Alice has cat." into the sequence „Cat has Alice". $A^{i'}_{j}$ can be treated as encrypted message, which to be read require the key x^{i}, and $x^{i'}$ is the encrypted message.

This approach has a drawback, namely that the encrypted message size is mach smaller than the size of transformation matrix $A^{i'}_{j}$. But the way of forming the transformation matrix $A^{i'}_{j}$ gives a chance to encrypt many messages with several keys. This significantly hamper the process of breaking the code, because without the knowledge of proper key it is not known, which of encrypted message is correct. From the other side, we can encrypt many messages devoted to different recipients, to be recognized based on possessed key.

Finding the transformation matrix $A^{i'}_{j}$ without knowing all the x^{i}_{n} or $x^{i'}_{n}$ is very difficult. However, knowing the transformation matrix $A^{i'}_{j}$, we can find the inverse

transformation matrix A_i^j evaluating the inverse matrix of $A_j^{i'}$. It is possible thus to recover all the keys based on knowledge of all encrypted messages. This operation is possible, however, when it is possible to calculate the inverse matrix of A_i^j, i.e. subject to condition $\det\left(A_j^{i'}\right) \neq 0$. If we insist on making impossible to recover the keys, based on encrypted messages, it suffices they form a linearly dependent set of vectors, i.e. two keys should decode the same message. In such a case, it is theoretically impossible to determine any key, based on encrypted information.

Conclusions

Generalized form of transformation makes possible to encrypt simultaneously many messages in one data sequence. Each encrypted message is related to one key. Having the relevant key, we can read the related message. This can significantly hinder operation of decoding algorithms, because we encrypt true massage as well as false message. In such case, it will be impossible to decide, without knowing the relevant key, which of the messages is true. Subject to the condition $\det\left(A_j^{i'}\right) \neq 0$, it is not possible theoretically either to recover one of the key based on knowing the other key or encrypted message.

Bibliography:

1. Chor B., Rivest R. L.: *A knapsack type public key cryptosystem based on arithmetic in finite fields*, In Proceedings of CRYPTO 84 on Advances in cryptology, pages 54–65, New York, NY, USA, 1985. Springer-Verlag New York, Inc.
2. Diffie W., Hellman M. E.: *New directions in cryptography*. IEEE Transactions on Information Theory, IT-22(6):644–654, 1976.
3. Hoffstein J., Silverman J.H.: *A non-commutative version of the NTRU public key cryptosystem*, 1997.
4. Jain A. K.: *Fundamentals of Digital Image Processing*, Englewood Clifs, Prentice-Hall International Inc., 1989.
5. Karaśkiewicz E.: *Zarys teorii wektorów i tensorów*, Warszawa: PWN, 1974.
6. Koblitz N.: *Elliptic curve cryptosystems*, Mathematics of Computation 48 (1987): 203-209, 1987.
7. Lim J. S.: Two-*dimensional signal and image processing*, Englewood Clifs, Prentice-Hall International Inc., 1990.
8. Merkle R. C., Hellman M. E.: *Public key cryptographic apparatus and method*, US Patent 4,218,582, 1980.
9. Miller V. S.: *Use of elliptic curves in cryptography*, In Lecture notes in computer sciences, 218 on Advances in cryptology—CRYPTO 85, pages 417–426, New York, NY, USA, 1986. Springer-Verlag New York, Inc.
10. Oppenheim A., Schafer R., Buck J.: *Discrete-Time Signal Processing*, International Edition 2nd Edition, 1999.
11. Raszewskij P. K.: *Rimanowa geometrija i tenzornyj analiz*, Moskwa, Nauka, 1964.

12. Rivest R. L., Shamir A., Adelman L. M.: *A method for obtaining digital signatures and public-key cryptosystems*, Technical Report MIT/LCS/TM-82, 1978.
13. Schroder H.: *One- and Multidimensional Signal Processing*, Chichester, John Wiley and Sons, LTD, 2000.