Contents of issue 2 vol. LVII

Engineering Transactions, Vol. **LVII**, No. 2, pp. 69–124, Warszawa 2009

ENGINEERING TRANSACTIONS • *Engng. Trans.* • **57**, 2, 71–87, 2009
Polish Academy of Sciences • Institute of Fundamental Technological Research

NUMERICAL ANALYSIS OF THE EFFECT OF TORISPHERICAL HEAD ON THE BUCKLING OF PRESSURE VESSEL

M. R. K h o s h r a v a n, A. R a h m a n i

University of Tabriz
Faculty of Engineering
Mechanical Engineering Department
Tabriz, Iran

The shape of end heads of a pressure vessel is usually torispherical. Buckling of this head is one of the most important points for designing of pressure vessels. This subject has been studied extensively since last years. In this field, the experimental methods are expensive and need a lot of time. In addition, because of lack of accuracy in the producing procedure, sometimes two models with identical geometry show different buckling behavior. Hence the use of finite element method in analyzing of buckling behavior of heads has a lot of benefits. In this dissertation, the finite element method has been used. Firstly with nonlinear buckling analysis, the effects of geometrical parameters such as thickness, knuckle radius and diameter of cylindrical part, on the buckling of heads have been studied, then the buckling behavior of different kinds of heads with identical geometry have been analyzed. For the nonlinear analysis we used the Arc Length method which can control the load level, the length of the displacement increment and the maximum displacement. The most important characteristic of this method is its ability to converge, even when the behavior is highly nonlinear. From the verification performed with the European Convention for Constructional Steelwork (ECCS) code, it has been confirmed that the nonlinear buckling analysis could assure accurate results for the buckling strength. In the case of internal pressure, it has been shown that initial imperfection had no effect on the pre-buckling behavior and buckling pressure of head; it just affects the post-buckling behavior.

1. Introduction

The theories of thin-walled structures applied on the pressure vessel were reviewed by Teng *et al.* [1]. Their results concerning linear and non-linear theories of thin-walled shells of revolution for numerical evaluation of buckling have been presented.

Regarding to existence of non-continuous stress distribution in cylinder-head intersection, the choice of head considering the geometrical limitation and production facilities is the most important point in designing of a pressure vessel.

Torispherical heads are used commonly in pressure vessels because of their simple manufacturing and good strength in high pressure conditions (Fig. 1). The buckling strength is one of the most important points in the design of pressure vessel [2]. Internal pressurization is often an important loading condition for pressure vessels. Finite element method is often used in the buckling analysis of pressure vessels due to its capability.

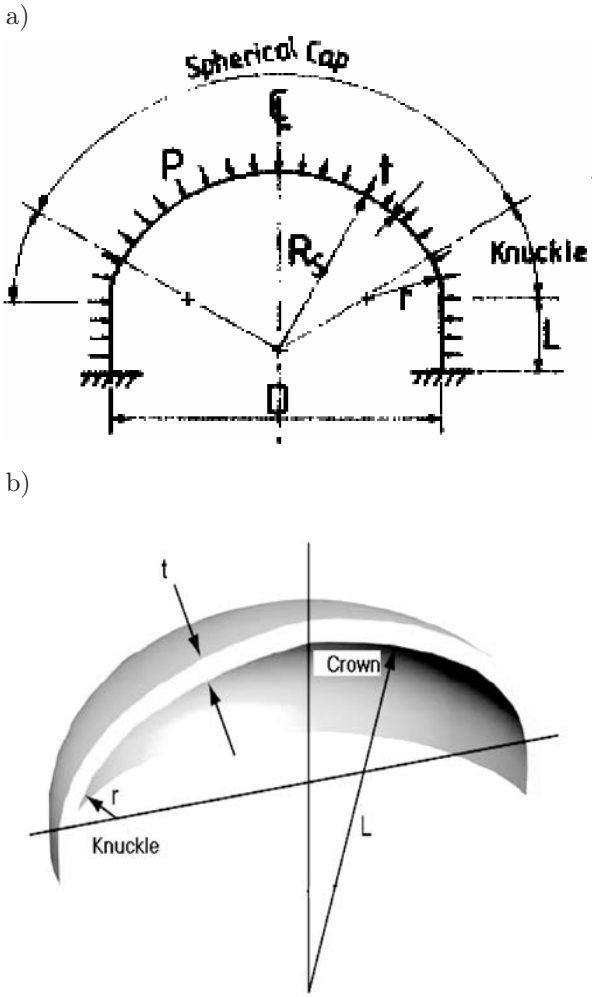

FIG. 1. Geometry of torispherical head. a) 2D-view with parameters and boundary conditions, b) view a the half-crown.

The hydrostatic buckling of shells under different boundary conditions (B.C.) has been investigated using the energy method [3]. Results have shown that in shells with medium height under different B.C., buckling load is obtained by

applying a scalar coefficient to the buckling load of the pin-ended case, but this method is not applicable to the long shells, for which the circumferential waves occurred from buckling are higher than 3.

Teng *et al.* [4] have introduced a numerical model, aided by the method of eigenmode-affine, in the non-linear analysis of elastic shells. As the shells are sensitive to the initial geometric imperfections, predicting of their buckling resistance would be precise if those imperfections were taken into account.

In the torispherical heads, by increasing the ratio of knuckle radius per vessel diameter (r/D), dimension of the spherical part decreases. Thus, the spherical part as a part of the head becomes weaker and in a defined r/D, a notable fall in buckling resistance occurs [5].

European recommendation ECCS [6] introduced several experimental relations for design of spherical shells. In a recent analysis, Wanderlich [7] analyzed the buckling behavior of spherical shells under external pressure.

Here we will discuss the buckling load and influence of different parameters on it. We will try to suggest some propositions for limitation of buckling.

2. Numerical simulation methods

Buckling analysis can be carried out by numerical methods such as eigenvalue buckling analysis or non-linear buckling analysis, using the finite element approach. Eigenvalue buckling analysis predicts the theoretical buckling strength (the bifurcation point) of an ideal linear elastic structure. Bifurcation buckling refers to the unbounded growth of a new deformation pattern. Imperfection and material non-linearities can not be included in this analysis. Thus, the buckling strength obtained by eigenvalue buckling analysis may differ from that of a real structure and often yields unconservative results. Therefore, care is needed when using this method in actual evaluation of buckling strength.

Non-linear buckling analysis, including geometric and material non-linearities, is usually the more accurate approach and is therefore recommended for design or evaluation of actual structures. There are two methods for obtaining buckling strength by means of non-linear buckling analysis. One basic approach is to constantly increase the applied loads until the solution begins to diverge, which can be obtained by means of the load-controlled buckling analysis. Using this approach, a simple static analysis will be done, with large deflection extended to a point where the structure reaches its limit load. Another approach is to constantly increase the displacement to obtain the snap-through buckling curve shown in Fig. 2. Increasing of the displacement can be obtained from displacement-controlled buckling analysis. In non-linear buckling analysis, a sufficiently small load or displacement increment should be used to obtain the expected buckling strength.

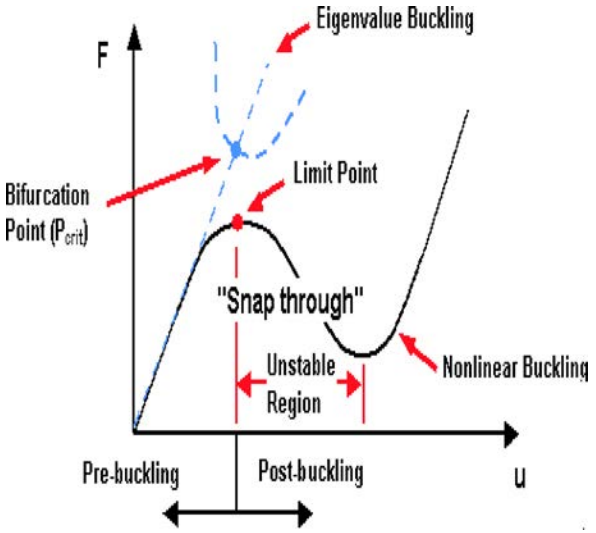

FIG. 2. Curve of non-linear buckling behaviour [8].

3. MODELING

Non-linear finite element method with large deflection analysis was performed using the commercial Ansys software. A three-dimensional finite element model was generated using Ansys 9.0 as shown in Fig. 3. To studying the buckling of pressure vessel with torispherical head, we modeled the intersection of cylinder-head. The influence of welding and forming on a material property were neglected while the effect of welding can be accounted for by modifying the yield stresses. The length of the cylinder was kept at 4λ (λ is the linear elastic meridional bending half-wave length given by $2.44\sqrt{Rt}$), to ensure that the boundary effects at the far end of the cylinder do not interfere with the behavior of the intersection [9]. The model was meshed by means of SHELL93 element. SHELL93 is particularly well-suited to model curved shells. The element has six degrees of freedom at each node: translations in the nodal x, y, and z-directions and rotations about the nodal x, y and z-axes. The element has the properties of plasticity, stress stiffening, large deflection and large strain capabilities. The material of the intersections was assumed to have typical properties of steel: an elastic modulus of 1.9×10^5 MPa; Poisson's ratio of 0.26, and yield stress of 206 MPa, and exhibits an elastic-perfectly plastic behavior.

For modeling of the geometrical imperfections in ANSYS package, we applied them in the form of initial deformations on the model [8, 10, 11]. For this reason, first we analyzed the model by using the linear method of buckling and then, by using the "Update Geom" order, we assumed the values of the magnification

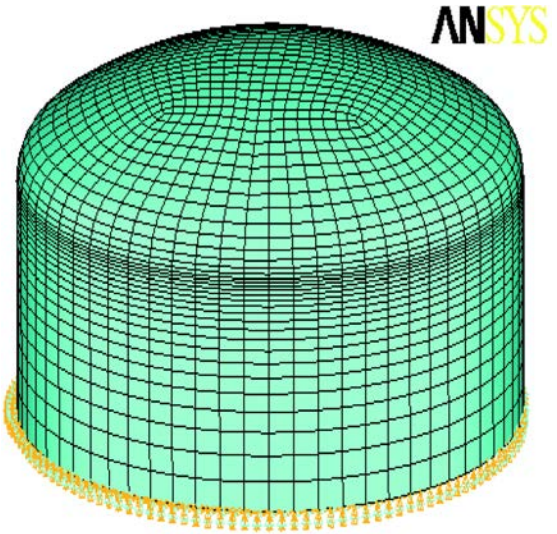

FIG. 3. Finite element model before buckling.

factor. In fact, by the resulting displacement of different buckling resolutions, a new model with geometrical imperfection was obtained. This factor of geometrical imperfection, which is in fact a deviation from the perfect model or the initial deformation, was presented by W_0. The buckled model is illustrated in Fig. 4.

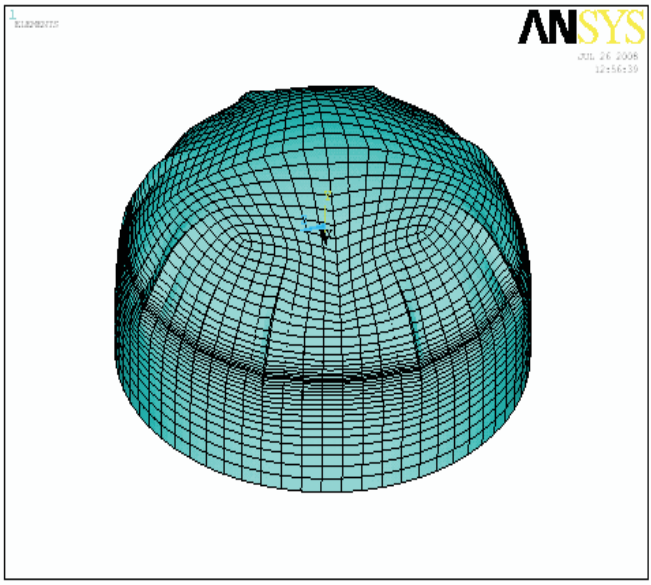

FIG. 4. Finite element model after buckling.

4. Choice of the resolving method

For the solution of a nonlinear problem, the choice of solution method and load step (referred to as the time step in the ANSYS software), is very important. It should take into account the anticipated structural behavior and the characteristics of the specific solution method.

Prior to carrying out a nonlinear buckling analysis, it is often beneficial to undertake a linear (eigenvalue) buckling analysis, in order to obtain some appreciation of the buckling behavior. It may also help to identify those regions in the model that will first exhibit nonlinear response, and at what load levels these nonlinearities will develop.

There are several methods available in ANSYS for the solution of the nonlinear buckling equations. They include the Newton–Raphson and Arc Length methods. For geometrically nonlinear analysis, the Newton–Raphson method has been shown to be one of the best methods available. The most important characteristic of this method is its ability to converge even when the behavior is highly nonlinear. The method we start with is also extremely accurate and generally converges quite rapidly, provided a realistic initial estimate of the displacement vector. With this method it is also possible to control the solution error and estimate the rate of convergence, since for any particular load step, the iterations continue until the specified solution error is achieved. Preliminary ANSYS FE analyses of the columns, in which compression loads were applied, showed that the Newton–Raphson method converged quite rapidly. For the nonlinear buckling analysis, coarse time steps may be used in the pre-buckling regime, but fine steps are required close to the buckling load and in the post-buckling regime. Different time steps may be used in the pre- and post-buckling regimes through the multiple 'load steps' option within ANSYS. However, it is not easy to choose the appropriate maximum load level in load-controlled analysis using the Newton–Raphson method.

Moreover, the Newton–Raphson method fails when a snap-through occurs. The Arc Length method does not have this drawback and allows one to control the load level, the length of the displacement increment and the maximum displacement. Therefore, in the nonlinear buckling analyses, the Arc Length method was used [12].

5. Determination of the buckling pressure

The Southwell plot technique is usually an effective approach in determining of the buckling load of the corresponding perfect structure [11]. This method was also adopted in this study, but unfortunately, it was not found to be ap-

plicable to our problem. The reason is probably that in our research, the load-displacement curves did not have generally the rectangular hyperbolic nature, which is basically necessary for application of the Southwell method. In our study we used a similar method as Theng's study on the cone-cylinder intersection [9]. In this approach, the curves of load-displacement for nodes in one circumferential path near the cylinder-head intersection were plotted. In the initial stage of loading, the curves for all nodes were similar, indicating a dominantly axi-symmetric behavior. As the pressure reached a certain value, the curves of nodes at different locations started to diverge from each other. The divergence of these curves is an indication of the growth of non-symmetric buckling deformations. The load corresponding to the divergence point is the critical buckling load (Fig. 5).

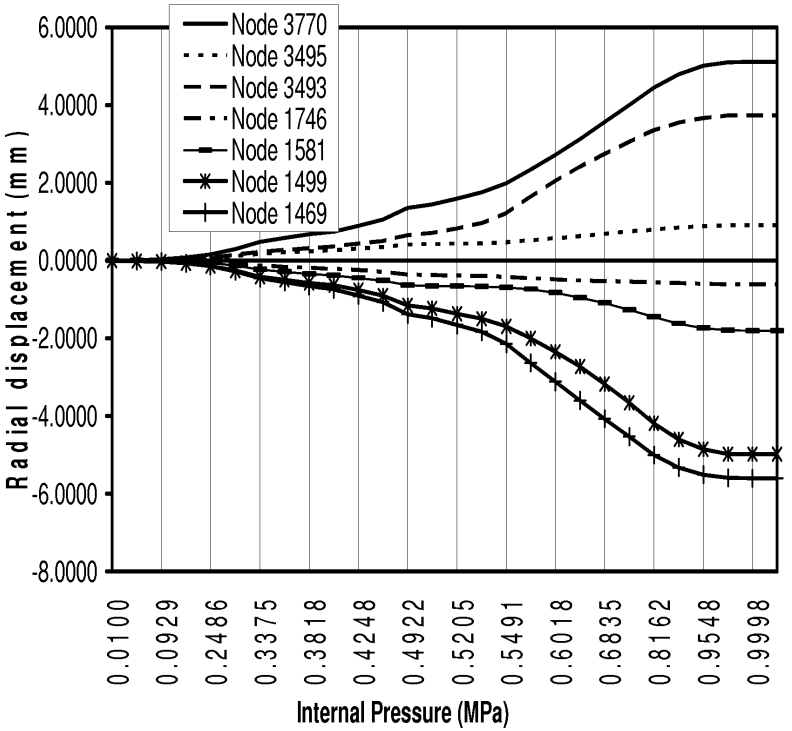

FIG. 5. Determination of buckling pressure (curve of load-radial displacement for torispherical head; $t/L = 0.002$, $r/L = 0.06$).

6. Parametric study

The geometry of torispherical head was introduced with the t/L, L/D and r/L parameters, in which t is the thickness of vessel which has identical values in

heads and cylindrical part, L is the radius of spherical section, r is the knuckle radius and D is the diameter of cylindrical section. The common heads used for pressure vessels which have radii of sphere equal to diameter of the cylinder ($L/D = 1$). Our study was limited to heads with

$$t/L \leq 500 \qquad \text{and} \qquad r/L \geq 0.06.$$

The result was compared with the design rules given in European Convention for Constructional Steelwork (ECCS) [6]. The ECCS rules are based on buckling of the knuckle and the limit pressure is as given in Eq. (6.1):

$$\frac{P_b}{F_y} = \frac{120c\left(\dfrac{r}{D}\right)^{0.825}}{(D/t)^{1.5}\left(\dfrac{L}{D}\right)^{1.15}}, \tag{6.1}$$

where $c = 1.0$ for crown and segment steel heads and $c = 1.6$ for cold-spun steel heads.

By verification performed with the ECCS code, as Table 1, Fig. 6 and Fig. 7 illustrate, it was confirmed that the nonlinear buckling analysis could assure accurate results for buckling strength. The discrepancy between the numerical analysis (FE) and ECCS [6] correspond to the geometrical imperfection and residual stress, which were taken into account by the ECCS code and not by the FE.

Table 1. Buckling pressure of vessel with torispherical head ($L/D = 1$).

t/L	r/L	P_{Ansys} (MPa)	P_{ECCS} (MPa)	Error %
0.002	0.06	0.20872	0.179	16
	0.08	0.22807	0.276	9
	0.1	0.34149	0.332	2.8
	0.14	0.43883	0.438	0.09
	0.17	0.48337	0.514	5.9
	0.2	0.542663	0.588	7
0.003	0.06	0.397296	0.400	0.67
	0.08	0.46551	0.507	8
	0.1	0.53235	0.610	12.7
	0.14	0.8196	0.805	1.7
	0.17	0.95637	0.944	1.2
	0.2	1.058	1.08	1.9

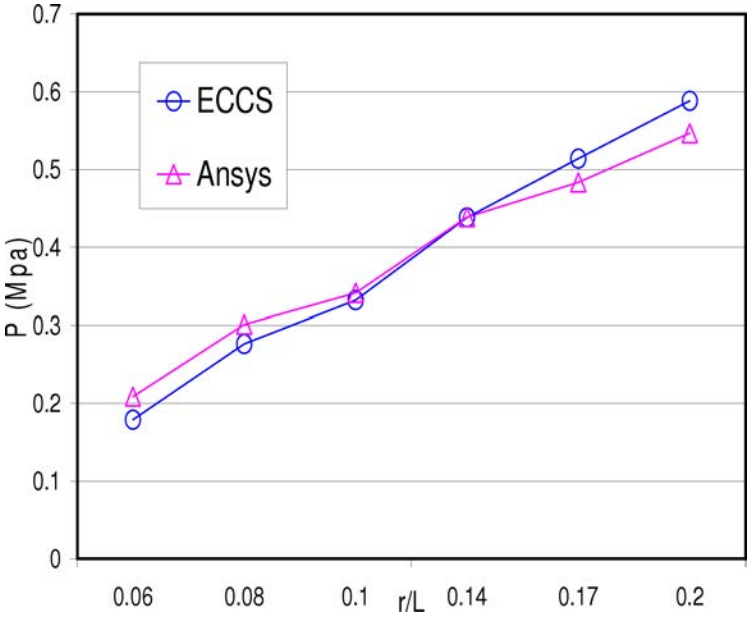

FIG. 6. Curve of critical pressure versus r/L ($t/L = 0.002$).

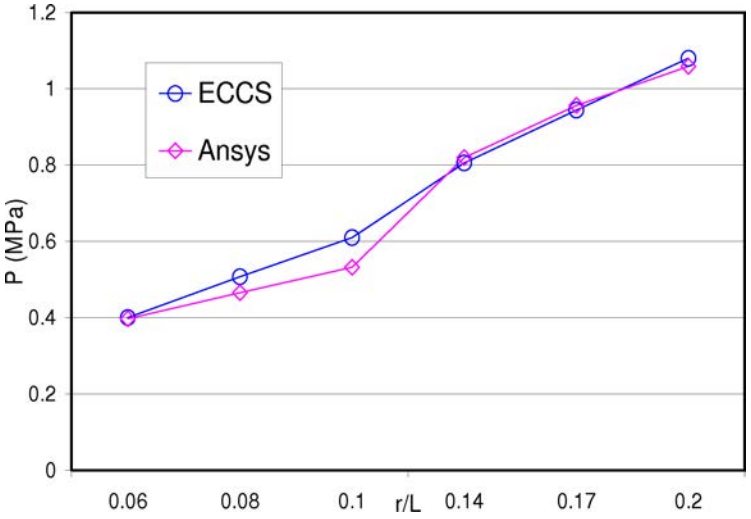

FIG. 7. Curve of critical pressure versus r/L ($t/L = 0.003$).

6.1. Influence of knuckle radius on buckling pressure

In the internal pressure vessels, due to the existence of circumferential tensile stresses in both the cylindrical and spherical parts, the intersection is deformed

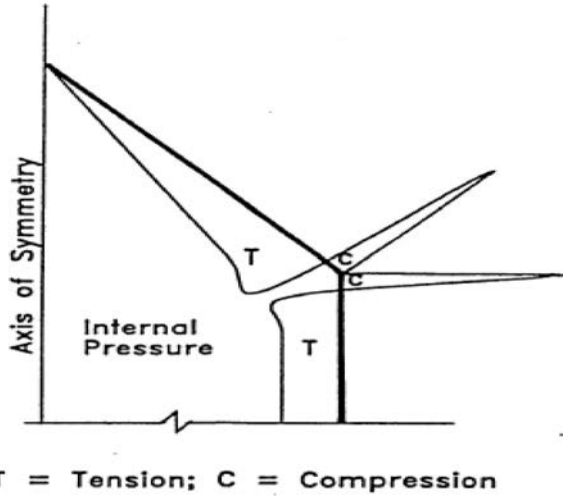

FIG. 8. Circumferential membrane stress in intersection [13].

to the internal side. Thus, both of the spherical and cylindrical parts near the intersection, as illustrated in Fig. 8, was subjected to circumferential compressive stresses, and so the buckling deflection occurred in both of them.

Figure 9 shows the buckling modes predicted by finite element analysis for the sphere-cylinder intersection with $t/L = 0.002$ and $r/L = 0.06$. These deformations are periodic around the circumference.

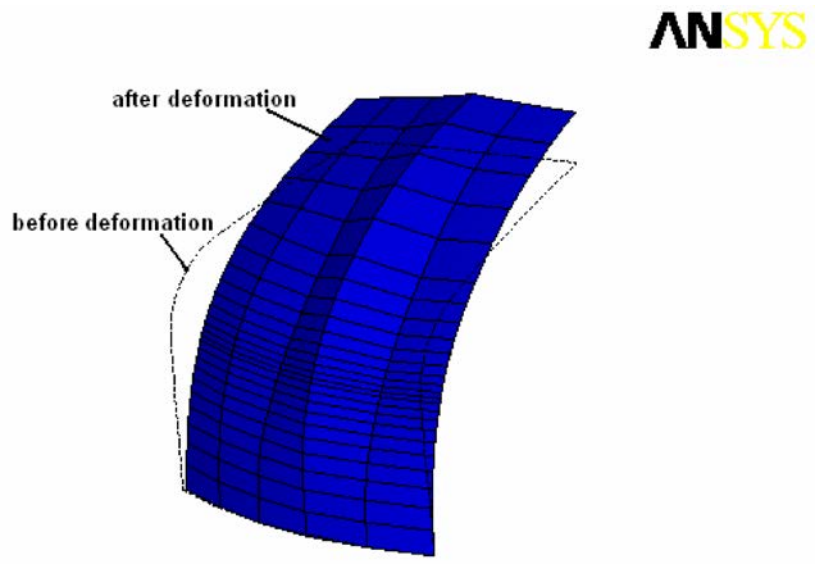

FIG. 9. Buckling modes.

The growths of buckles can now be clearly seen in Fig. 10. The number of periodic waves on the ring can be counted from this plot to be 39. It should be noted that this counted number is only a rough indication, as the buckling waves are not so uniform.

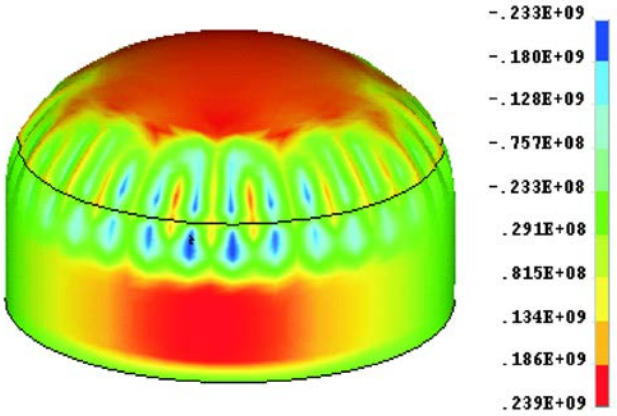

FIG. 10. Influence of knuckle radius ($t/L = 0.002$ and $r/L = 0.06$).

Numerical results for all the points of intersection between the head and cylinder have shown clearly that the post-buckling behavior of internally pressurized sphere–cylinder intersections is stable (Fig. 10).

The curves of Fig. 11 show the influence of knuckle radius on the pressure buckling with different thicknesses. In the analysis, the value of the radius of

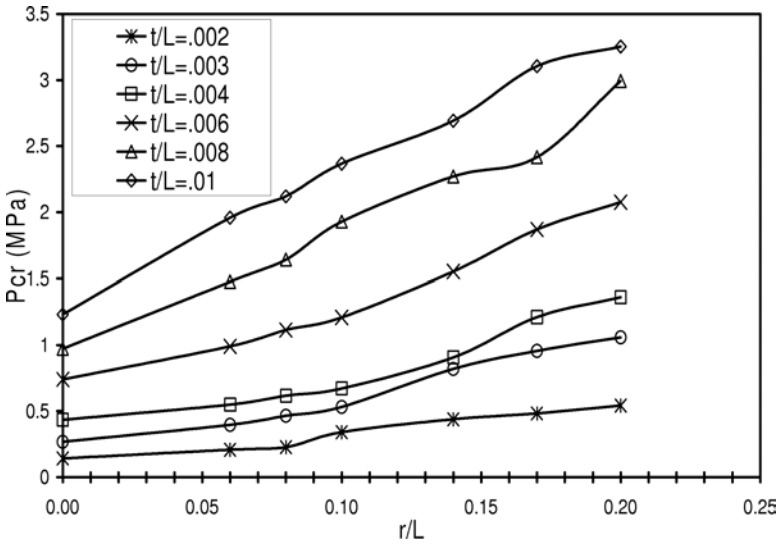

FIG. 11. Influence of the knuckle radius on the buckling behavior of the torispherical head.

spherical part (L) was kept constant ($L = 0.5$ m). When varying the ratio r/L, only the knuckle radius (r) was varied. We observe that for all the thicknesses, increasing of a radius leads to increasing of the buckling pressure. So the knuckle radius is an influential parameter for increasing of buckling resistance.

6.2. Influence of the thickness on the buckling pressure

Figure 12 illustrates the influence of t/L on the buckling pressure for different ratios of r/L. Increasing of t/L leads to increasing of the buckling pressure. The rate of increase, compared to increasing resulting from the ratio r/L, is higher. The slope of the curves of Fig. 12 as compared to those of the Fig. 11 shows it. Thus the buckling pressure is more sensitive to the thickness.

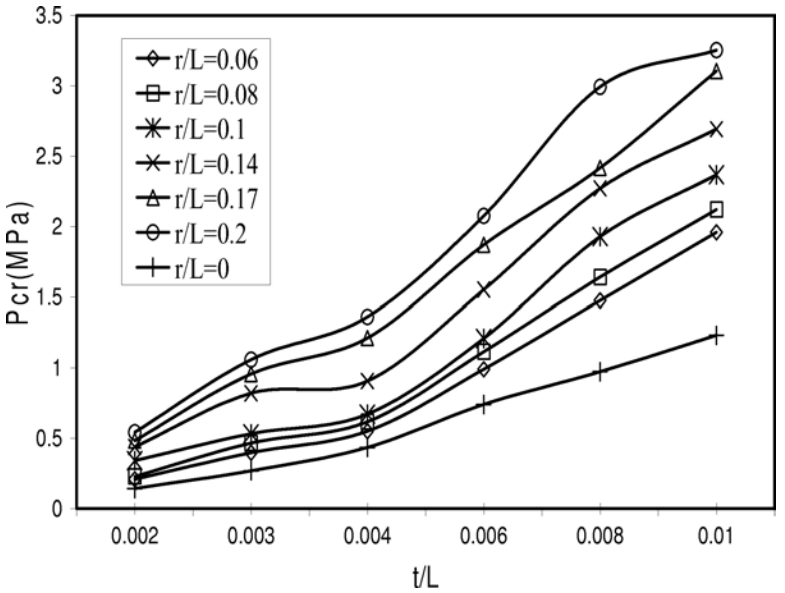

FIG. 12. Influence of t/L on the buckling pressure of the torispherical head.

6.3. Influence of the radius of the spherical part on the pressure buckling

In torispherical heads, usually the radius of sphere is the same as the cylinder ($L/D = 1$). Buckling of this kind of heads is discussed empirically. For the heads with different radii mentioned, result of FE for different ratios of L/D is shown in Fig. 13. The curve shows that by increasing of the radius of the spherical part, the buckling pressure decreases. So by decreasing of the curvature of the crown, the buckling pressure of the vessel decreases. In the same way, buckling pressure of the vessels with a plate head is much lower than of the vessels with a clear spherical head.

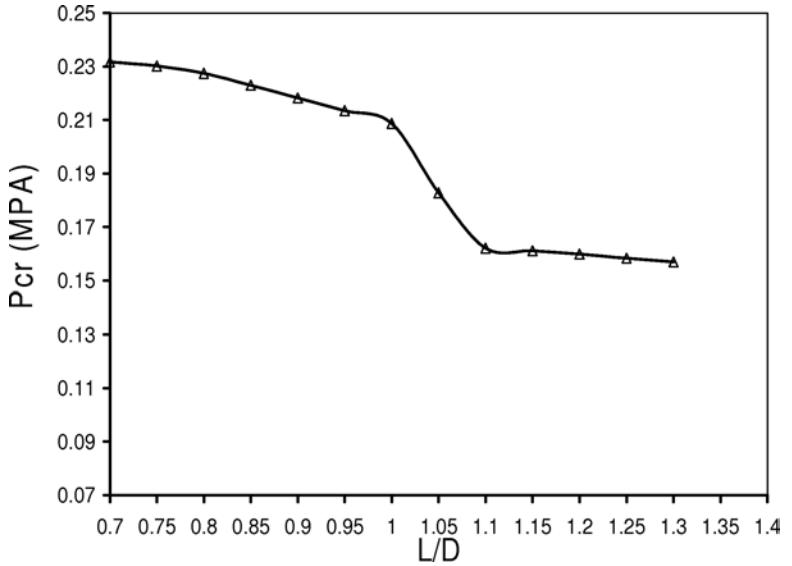

FIG. 13. Curve of the buckling pressure versus L/D for torispherical head.

While these observations may suggest that the direct use of bifurcation loads in design may be somewhat unconservative, a closer examination of the results has revealed that for many of these intersections, the plastic limit load of Eq. (8.1) is lower than the one-third stiffness load, or both the one-third and half-stiffness loads. This indicates that the strengths of these intersections are controlled by the plastic limit load, and the fact that the bifurcation load exceeds the stiffness-based buckling loads is not of a real concern. The direct use of the bifurcation loads in design is therefore generally safe.

7. Choice of the equivalent geometric imperfections

For a numerical buckling analysis it is essential, that well comparable and most general applicable equivalent imperfections should be used. To achieve this, the shape and the amplitude of the applied equivalent geometric imperfections have to reflect the effect of the really existing initial imperfections. But currently, there are no sufficient guidelines for the imperfection parameters of a numerical analysis. In [5] it is only stated, that the pattern of the equivalent geometric imperfection shall be chosen in such a form which leads to the most unfavorable effect in the buckling behavior of the shell. The 'worst' imperfection is not specified in detail and presently, no practically verified theory exists, which could indicate it. If the instability problem is caused by geometrical nonlinearity and the prebuckling behavior is almost linear, the eigenmode-affine imperfec-

tion patterns, which are derived from the classical linear eigenvalues analysis, are applicable. Besides the fact that these imperfections are unrealistic, we use eigen-affine imperfection in our study.

8. Results and discussion

8.1. Analysis of development of the circumferential wrinkles

Due to the buckling, circumferential wrinkles are developed. The number and amplitude of theses wrinkles increase by increasing of the internal pressure. The number and amplitude of the developed wrinkles are a criterion to evaluate the buckling resistance [14]. Creation and development of wrinkles could be followed by a curve of radial displacement versus the distance in a circumferential path, in the vicinity of intersection of the cylinder and head of the vessel (Fig. 14). Although by accounting of the number of wrinkles in this curve, the number of circumferential wrinkles in the head could be obtained.

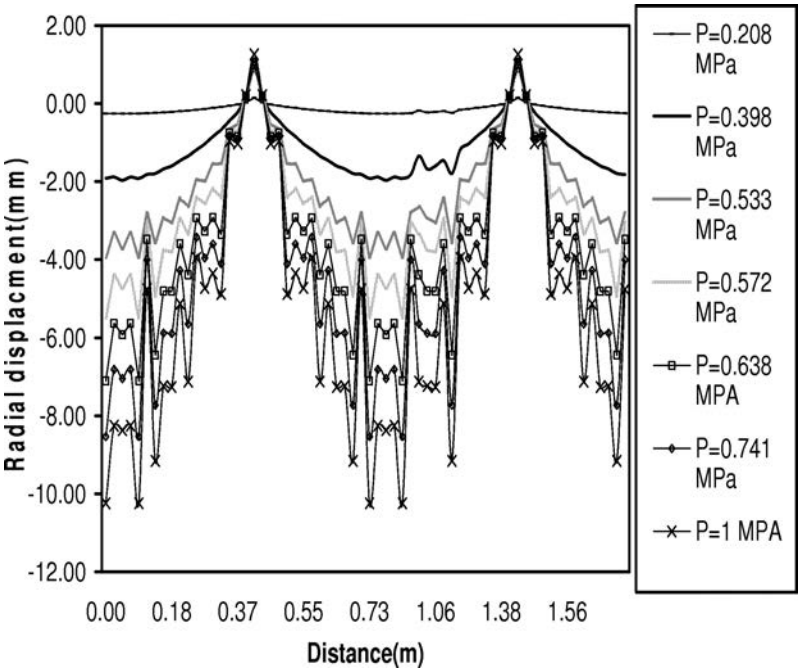

Fig. 14. Development of buckling wrinkle $r/L = 0.06$ and $t/L = 0.002$.

8.2. Comparison of buckling pressure with limit pressure

The limit pressure of the vessel (P_L) with torispherical head is computed using Eq. (8.1) [15] derived by Shield and Drucker [16]:

$$\frac{P_{SD}}{F_y} = \left(0.33 + 5.5\frac{r}{D}\right)\left(\frac{t}{L}\right) + 28\left(1 - 2.2\frac{r}{D}\right)\left(\frac{t}{L}\right)^2 - 0.0006, \tag{8.1}$$

in which P_{SD} is the limit pressure (psi), $P_{SD} = P_L$, F_y is the yield stress (ksi).

Figure 15 shows the critical buckling pressure (P_{cr}) versus the pressure obtained from Eq. (8.1). The curve shows that the buckling pressure is most often higher than the limit pressure. It means that the limit pressure is more critical than the buckling pressure. Thus for the vessels with torispherical head, the buckling pressure as a design criterion will not be sufficient.

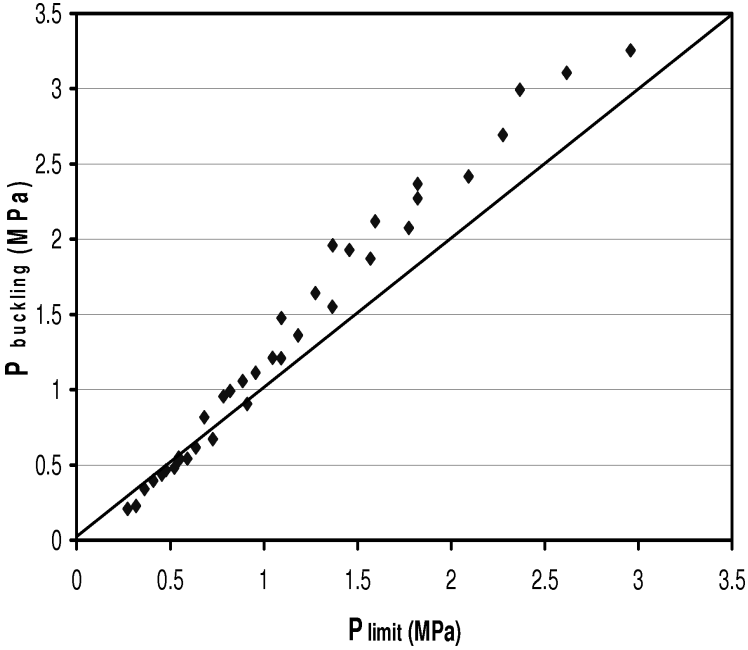

FIG. 15. Curve of buckling pressure versus limit pressure.

8.3. Influence of initial geometrical imperfection on buckling behavior

The analysis of imperfection sensitivity was performed with the initial imperfection values of $W_0/t = 1$, $W_0/t = 0.2$ and $W_0/t = 0.5$. The perfect model had $t/L = 0.002$ and $r/L = 0.06$. The buckling loads of all imperfect models, as illustrated in Fig. 16, were equal to the buckling load of the perfect model and had $P_{\rm cr} = 0.2087$ MPa. But the post-buckling behavior of imperfect models was different from post-buckling of the perfect model. The nearly perfect model ($W_0 = 0.2$) had the same value as the buckling load and the post-buckling behavior was such a perfect model. For the most imperfect model ($W_0 = 1$), the post-buckling behavior had the most important deviation from the perfect model.

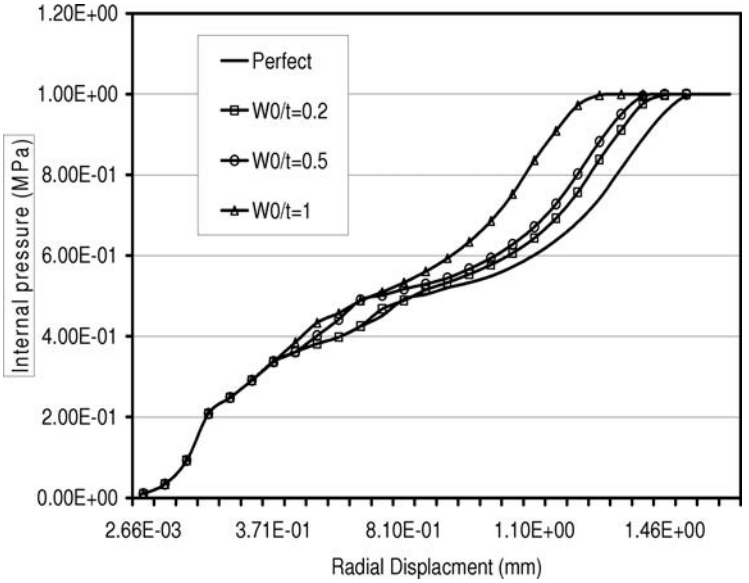

FIG. 16. Influence of imperfections on the buckling behavior.

The buckling pressure of all imperfect models being 0.208 MPa, we can conclude that imperfections do not influence the critical buckling pressure and pre-buckling behavior of the vessel. Only the post-buckling behavior is influenced by imperfections. Thus the buckling behavior of pressure vessels with torispherical head, because of their stable behavior, is not sensitive to initial geometrical imperfections.

9. Conclusion

- The non-linear FE analysis brings the numerical results in vicinity of the experimental ones. Scatters are generally due to the geometrical imperfections and residual stresses in a vessel.
- Buckling pressure is influenced by the thickness and height of the vessel. Larger thickness and height lead to a better buckling resistance.
- The influence of knuckle radius in decreasing of the compression stresses and also increasing of the buckling pressure is evident.
- In the case of uniform internal pressure, the initial geometrical imperfections have a small influence on the pre-buckling behavior and buckling load of torispherical heads. Their influence is considerable on its post-buckling behavior.
- Using of the buckling pressure criterion in design of torispherical heads would be conservative.

References

1. J. G. Teng and T. Hong, *Non-linear thin shell theories for numerical buckling predictions*, Journal of Thin-Walled Structures, **31**, 89–115, 1998.
2. X. Wang, J. Xiao and Y. C. Zhang, *A method for solving the buckling problem of a thiheln walled sl*, International Journal of pressure vessels and piping, **81**, 907–912, 2004.
3. R. Pinna and B. F. Ronald, *Hydrostatic buckling of shells with various boundary conditions*, Journal of Constructional Steel Research, **56**, 1–16, 2000.
4. J. G. Teng and C. Y. Song, *Numerical models for nonlinear analysis of elastic shells with eigenmode-affine imperfections*, International Journal of Solids and Structures, **38**, 3263–3280, 2001.
5. J. Blachut, *Buckling of sharp knuckle torispheres under external pressure*, Thin walled structure, **30**, 1–4, 55–77, 1998.
6. European Convention for Constructional Steelwork ECCS, Technical Working Group 8.4 [Ed.], Buckling of steel shells, European Recommendation, 4th Edition, ECCS, Brussels 1998.
7. W. Wunderlich and U. Albertin, *Buckling behavior of imperfect spherical shells*, International Journal of Non-Linear Mechanics, **37**, 589–604, 2002.
8. ANSYS Release 9.0, ANSYS Inc., 2003, Canonsburg, Pensylvania.
9. Y. Zhao and J. G. Teng, *A stability design proposal for cone-cylinder intersections under internal pressure*, Int. J. of Pressure and Vessel and Piping, **80**, 5, 297–309, 2003.
10. S. Kenny, N. Pegg and F. Taheri, *Dynamic elastic buckling of a slender beam with geometric imperfections subject to an axial impulse.* Finite element in analysis and design, **35**, 227–246, 2000.
11. V. P. Veedu and L. A. Carlsson, *Finite-element buckling analysis of sandwich columns containing a face/core debond*, Composite Structures, **69**, 143–148, 2005.
12. G. J. Turvey and Y. Zhang, *A computational and experimental analysis of the buckling, post-buckling and initial failure of pultruded GRP columns*, Journal of Computers and Structures, **84**, 1527–1537, 2006.
13. J. G. Teng, *Elastic buckling of cone-cylinder intersection under localized circumferential buckling*, Journal of Engineering Structure, **18**, 41, 1996.
14. J. G. Teng and M. Hong–Wei, *Elastic buckling of ring-stiffened cone-cylinder intersections under internal pressure*, ASME International Journal of Mechanical Science, **41**, 357–383, 1999.
15. C. D. Miller, *Buckling criteria for torispherical heads under internal pressure*, International Journal of Pressure Vessel Technology, **123**, 318–323, Aug. 2001.
16. R. T. Shield and D. C. Drucker, *Design of thin-walled torispherical and toriconical pressure vessel heads*, ASME Int. Journal of Applied Mechanics, **28**, 292–297, 1961.

Received October 14, 2008; revised version September 5, 2009.

ENGINEERING TRANSACTIONS • *Engng. Trans.* • **57**, 2, 89–104, 2009
Polish Academy of Sciences • Institute of Fundamental Technological Research

ON IMPROVED IMAGE ENCRYPTION SCHEME BASED ON CHAOTIC MAP LATTICES

K. Jastrzębski [1)], Z. Kotulski [2)]

[1)] **Warsaw University of Technology**
Department of Electronics and Information Technology
Nowowiejska 15/19, 00-665 Warszawa, Poland

[2)] **Institute of Fundamental Technological Research**
Polish Academy of Sciences
Pawińskiego 5B, 02-106 Warszawa, Poland

In this paper we examine one of the recently proposed chaotic image encryption algorithms, based on chaotic map lattices (CML). We show certain problems with the chaotic map, as well as errors in the designed algorithm. Then we propose a way to improve it and present a new version of algorithm and its implementation. At the end, we show the results of a security analysis and a comparison of both schemes. These results were obtained in the MSc Thesis [25].

Key words: Discret Chaotic Cryptography (DCC), image encryption, chaotic dynamical systems.

Chaotic dynamical systems were independently identified by Edward Lorenz and Yoshisuke Ueda in 1961. They started to be involved into secure communication in the 9th decade of the 20th century. First, the chaos-based security research was concentrated on continuous (in time) dynamical systems, governed by nonlinear differential equations, and two techniques: chaos control and chaos synchronization. Such techniques are useful for secure streaming, analogous to stream ciphers known in traditional cryptography. Then, discrete dynamical systems were applied in a way analogous to block cipher encryption. The second technique started to be extensively studied when it was applied to image encryption, which needs very efficient algorithms (due to large sets of bits representing multicolor pixels). In this paper, we propose an algorithm that could satisfy expectations of efficiency and security in a case of image encryption, both black and white and color.

1. Introduction

Discrete chaotic dynamical systems are nonlinear, exponentially sensitive to changes of initial conditions, the points of their trajectories take values from

uncountable sets and their subsets of phase space, while the systems are ergodic or mixing, are equiprobable and asymptotically statistically independent. Moreover, chaos may occur even in simple recursive equations. These properties are very good from cryptographic point of view, which was intuitively described even by SHANNON [1], when he was introducing the concept of mixing in the information theory field. Analogies between features of chaotic systems and properties of good cryptosystems are widely known [2–4]. The main problem, still unsolved is how to transfer chaos into finite-state space-valued digital systems, see [5]. Despite this, scientists are still trying to find a cryptographic application of mathematical tools of the chaos theory. Many ideas concentrate on ciphers based on discrete (in time) chaotic maps.

The first cipher of this class was proposed in 1991 by HABUTSU *et al.* [6]. The transformation used was a tent map, a plain text was an initial condition and a key was the map control parameter, which placed the top of a tent. This cipher was easily broken [7]. The second idea was to insert the key into the initial condition of a dynamical system, proposed by KOTULSKI and SZCZEPAŃSKI [8]. Afterwards, BAPTISTA [9] suggested a cryptosystem, in which both the initial condition and the control parameters played a role of a secret key. In the next cryptosystem, [10], the inspiration was a thermodynamical model of a gas particle, closed in a container, which is subject to a chaotic reflection law. This time the map was two-dimensional and the key was one of the two initial conditions. d-dimensional dynamical systems (previously agreed between communication sides) were a base of the cryptosystem introduced by ALVAREZ *et al.* [11]. In all of these systems the number of iterations of a chaotic map was limited on the one hand by the condition of obtaining a statistically good ("random") ciphertext, on the other hand by the time of computation. These conditions, the way of using the map and described forms of the key became typical for most of the proposed ciphers. A more detailed review of propositions may be found [12].

There are attempts to apply discrete in time, chaotic systems also in image encryption. Image encryption is connected with some specific problems [13], such as: huge redundancy and size of data, strong correlation between pixels, compression, different significance of bits (to human eye), speed of computation (sometimes more important than high security level), etc. In many applications, conventional encryption schemes are not suitable [14]. Consequently, many scientists turned their attention to algorithms specifically designed for image and video encryption and to be fast, including many chaotic encryption propositions (e.g. SPIHT algorithm [15], CKBA [16], BRIE [17], cipher based on 3D Baker's transformation [18], RRS-CVES [19]). There exist two approaches: the first one is to use chaos to permute the order of the pixels; the second one is based on changing the numerical values responsible for the color of each pixel. There appeared also some ideas to join these two operations, calling them the confusion

phase and the diffusion phase [20]. The level of sophistication among the propositions on a secure chaotic cipher constantly grows, although most algorithms turned out to be insecure (a detailed review [12]). One of the latest propositions is the image encryption algorithm based on chaotic map lattices (CML) [21]. This cipher is the starting point of our paper.

The scheme of the paper is the following. Section 2 presents the original CML algorithm. In Sec. 3 we point out some problems in this proposition. Next (in Sec. 4), we introduce modifications, which improve the CML scheme. In Sec. 5 we present a security analysis of the modified algorithm. In the last Sec. 6 we draw conclusions and show the direction of future works.

2. CML image encryption scheme

As it was mentioned, image encryption hides some specific problems, such as huge redundancy and size of data or required effectiveness. Some scientists believe that chaotic ciphers will turn out to be a good solution to these problems. An interesting proposition is the CML scheme [21]. This algorithm has features similar to *cipher-block-chaining* (CBC) mode, known from the block ciphers theory [22]; here blocks are pixels. It means that the encrypted value of a pixel depends not only on the value of the pixel itself but also on the values of cryptograms of its neighbors. Such a property is especially important for image encryption because any ECB mode (*electronic code book* mode, where identical pixels are identically encrypted) does not hide contours of elements of a picture.

As a map, CML uses the logistic equation:

$$x_{n+1} = a x_n (1 - x_n), \tag{2.1}$$

where $a \in (3.57, 4.00)$ is the control parameter. For all values of a there exist uniquely determined values $x_{\min}$ and $x_{\max}$, such that in successive iterations the values of the variable x_n don't leave the range of $[x_{\min}, x_{\max}]$. Let us also define $\delta x = x_{\max} - x_{\min}$.

Input data of the cipher are pixel matrices, i.e. three matrices of color components in RGB coding, where each element of the matrix takes a value from 0 to 255. If the image is monochromatic, there is obviously one matrix of numbers (grayscale values). The value of each color component of the pixel is used as initial value for the logistic equation. Conversion to floating-point numbers and back to colors are realized by formulas:

$$x_c = x_{\min} + \delta x \left(\frac{C_c}{255} \right), \tag{2.2}$$

$$C_c = round \left((x_c - x_{\min}) \frac{255}{\delta x} \right), \tag{2.3}$$

where $c = \{R,\ G,\ B\}$, C_c is the c-th component of the color C, and x_c is its floating-point value. The Eq. (2.3) should guarantee returning to the $\{0,\ 1,\ \ldots,\ 255\}$ set, thus colors of pixels.

Encryption procedure

Let the plain image contain $N \times M = m$ pixels, and let $i = 1,\ 2,\ \ldots,\ m$ be a pixel index. To make the description simpler, let us assume that the image is black and white, represented by one matrix of numbers.

At the beginning, all pixels are changed to floating-point numbers, according to Eq. (2.2). The value of m-th pixel is taken as an initial condition for the map, i.e. $x_0^1 = x_c^m$. The value obtained from the map after n iterations is added to the value of the first pixel x_c^1, i.e. $x_c^1 + x_n^1 = x_c^1 + M^n\left(x_0^1\right)$. If the sum exceeds $[x_{\min},\ x_{\max}]$, it has to be normalized by subtracting δx. The obtained result is overwritten as a value of the first pixel. This value becomes a new initial condition for the map, which is iterated n times, and the obtained result is added to the next pixel. The sum, if necessary, is normalized and overwritten on the next pixel's place and so on. The described procedure is carried through all pixels and repeated j times for the entire image. Using Eq. (2.3) we convert numbers to grayscale shades. If we have a color image, the algorithm is done subsequently to all three RGB matrices.

The algorithm proposed in [21], in a more formal way, may be presented as:

Algorithm 1. CML cipher encryption procedure.

Input:
- j – number of cycles, part of a cipher key
- m – number of pixels, part of a cipher key
- IMG – stream of image pixels
- n – number of iterations, part of a cipher key
- M – chaotic map
- p – control parameter, part of a cipher key
- $x_{\min},\ x_{\max}$ – borders of the attractor, dependent on p
- $\delta x = x_{\max} - x_{\min}$

Output: stream of encrypted pixels

1. **for** $pixel \leftarrow 1$ **to** m **do** $IMG(pixel) \leftarrow x_{\min} + \delta x \dfrac{IMG(pixel)}{255}$
2. **for** $cycle \leftarrow 1$ **to** j **do** steps from 3 to 7
3. **for** $pixel \leftarrow 1$ **to** m **do** steps from 4 to 7
4. $x_0 \leftarrow IMG(pixel\ - 1)$
5. **for** $i \leftarrow 1$ **to** n **do** $x_i \leftarrow M(x_{i-1}, p)$
6. $IMG(pixel) \leftarrow IMG(pixel) + x_n$
7. **if** $IMG(pixel) > x_{\max}$ **do** $IMG(pixel) \leftarrow IMG(pixel\ ) - \delta x$
8. **for** $pixel\ \leftarrow 1$ **to** m **do** $IMG(pixel) \leftarrow round\left((IMG(pixel) - x_{\min})\,\dfrac{255}{\delta x}\right)$

As a pixel preceding the first one, the last image pixel is taken.

The secret key of the algorithm consists of four numbers: the control parameter a, the number of iterations n, the number of cycles j and the size of the image $m = N \times M$, i.e. the tuple $\{a,\ n,\ j,\ m\}$.

Decryption procedure

Again, let us assume for simplicity, that the encrypted image is black and white.

Firstly, to recover the original image, pixels of ciphertext should be converted to a matrix of floating-point numbers. Then, from the value of m-th pixel we subtract the value of the previous pixel, which was earlier iterated n times on the chaotic map. If the result is less than 0, it should be normalized by adding δx. These operations are repeated for all pixels of the image, remembering about the assumed condition for the last pixel. The whole image is processed j times. If we have a color image, we expand the algorithm in a way analogous to the encryption procedure.

The decryption algorithm may be presented more formally as:

Algorithm 2. CML cipher decryption procedure.

Input: j – number of cycles, part of a cipher key
m – number of pixels, part of a cipher key
IMG – stream of encrypted image pixels
n – number of iterations, part of a cipher key
M – chaotic map
p – control parameter, part of a cipher key
$x_{\min},\ x_{\max}$ – borders of the attractor, dependent on p
$\delta x = x_{\max} - x_{\min}$

Output: stream of decrypted pixels

1. **for** $pixel \leftarrow m$ **to** 1 **do** $IMG(pixel) \leftarrow x_{\min} + \delta x \dfrac{IMG(pixel)}{255}$
2. **for** $cycle \leftarrow j$ **to** j **do** steps from 3 to 7
3. **for** $pixel \leftarrow m$ **to** 1 **do** steps from 4 to 7
4. $x_0 \leftarrow IMG(pixel - 1)$
5. **for** $i \leftarrow 1$ **to** n **do** $x_i \leftarrow M(x_{i-1}, p)$
6. $IMG(pixel) \leftarrow IMG(pixel) - x_n$
7. **if** $IMG(pixel) < 0$ **do** $IMG(pixel) \leftarrow IMG(pixel) + \delta x$
8. **for** $pixel \leftarrow 1$ **to** m **do** $IMG(pixel) \leftarrow round\Big((IMG(pixel) - x_{\min})\,\dfrac{255}{\delta x}\Big)$

Again, as a pixel preceding the first one, the last image pixel is taken.

To achieve a reasonable security level, authors [21] recommend using the key values not smaller than: $n = 75$ and $j = 3$. Obviously, along with the growth of the both parameters, the computation time of the algorithm also grows. As

a remedy, the authors claim that it is possible to increase the security level, by simply using different values of a and n for each pixel. It does not increase the computation time significantly.

3. Certain problems with CML encryption scheme

The version of CML algorithm, presented in [21], unfortunately contains several mistakes and inaccuracies, which make the algorithm impossible for practical use. In this section we point out the observed inaccuracies of the algorithm.

There exists a problem with conversion from floating-point numbers to pixel colors in the algorithm. Using $round(\cdot)$ operator results in small information leakage and initial conditions for the map in the encryption device, and the decryption device are slightly different. Because of exponential sensitivity of chaotic maps, it makes a proper decryption of the original image impossible. Table 1 illustrates quantitatively this fact.

Table 1. Values of exemplary pixels in encryption device and decryption device as initial conditions, values obtained from them by using the logistic map with $a = 3.9$ and $n = 75$ and the error between these values. Slight differences grow exponentially and are unpredictable. Therefore, a proper decryption is impossible.

initial condition in encryption	initial condition in decryption	value from the map (encryption)	value from the map (decryption)	error	error percent [%]
0.457858	0.457389	0.957239	0.964287	0.007048	0.736
0.632534	0.629926	0.869645	0.904273	0.034628	3.982
0.694364	0.692040	0.103459	0.645242	0.541783	523.669
0.781274	0.778308	0.612869	0.319281	0.293588	47.904
0.811925	0.809365	0.155187	0.908149	0.752962	485.197
0.299123	0.298655	0.335547	0.910547	0.575000	171.362
0.258364	0.257247	0.732454	0.900507	0.168053	22.944
0.973357	0.971549	0.146878	0.974617	0.827739	563.556
0.375212	0.374572	0.098140	0.343083	0.244943	249.585
0.169265	0.167527	0.432184	0.097871	0.334313	77.354

It may be considered, whether the algorithm in authors' intention would not have worked in a different way: it were the floating-point numbers which should be transmitted, not the colors. Unfortunately, this form of algorithm means that the size of transmitted data grows (using floating-point variables) and that

the attack on the key-space is possible (we can easily extract extreme values from a ciphertext, which would be close to $x_{\min}$, $x_{\max}$, uniquely determining the parameter a).

There is also another problem. In order to have the floating-point values not exceeding the borders of an attractor, i.e. in the range of $[x_{\min}, x_{\max}]$, the normalization process was introduced (adding and subtracting δx). Unfortunately, the normalization process does not work properly, what is illustrated in Tables 2 and 3 (it was assumed that the encryption procedure encounters values close to the extreme).

Table 2. Result of executing the algorithm on the extreme values $x_{\max} = 0.9$ and $x_{\min} = 0.1$, with $\delta x = 0.9 - 0.1 = 0.8$. In the right down quarter we can see leaving the range of $[x_{\min}, x_{\max}]$, to which normalization ought to prevent.

$+$	**0.1**	**0.9**
0.1	0.2	$1.0 - \delta x = 0.2$
0.9	$1.0 - \delta x = 0.2$	$1.8 - \delta x = 1.0$

Table 3. Result of executing the algorithm on the extreme values $x_{\max} = 0.9$ and $x_{\min} = 0.1$, with $\delta x = 0.9 - 0.1 = 0.8$. In three cases we see 0, which means leaving the range of $[x_{\min}, x_{\max}]$, which normalization ought to prevent.

$-$	**0.1**	**0.9**
0.1	0.0	$-0.8 + \delta x = 0.0$
0.9	0.8	0.0

As we can see, with the values close to extreme, it occurs that normalization causes leaving outside the attractor.

Moreover, the algorithm brings some questions about the map. A dynamical system is chaotic, when it is mixing and has at least one positive Lyapunov exponent [23]. The logistic map is chaotic for control parameters $a > s_\infty$, where $s_\infty = 3.5699\ldots$ is the Feigenbaum point. Unfortunately, for the logistic map, even for many isolated values $a > s_\infty$, the Lyapunov exponents λ take negative values (a diagram of numerical calculations may be seen e.g. in [24]). To those a, chaos does not appear in the system and as we know, security of the cipher was based on chaos. What is more, using the chaotic map in finite precision is associated with a so-called dynamical degradation. It emerges as a result of quantization of state space of the mathematical system, which operates in the set equivalent with $\mathbf{R}$. This phenomenon causes appearing of short cycles and general worsening of statistical properties of a system [5, 12]. It may also be used to attack a chaotic cryptosystem [12].

In the CML algorithm, the size of the key-space depends on types of variables used in the implementation, which was not precisely defined by the authors. What is more, the range of parameters n and j is obviously limited and makes a small contribution to overall size of the key-space. Using different values of n and a for each pixel, which was suggested in [21], is not a good idea because of the large length of such a key.

4. An improved CML algorithm

Because of the problems described above, we try to show the direction of necessary changes in the CML algorithm. As a chaotic map we chose the 1D *piece-wise linear chaotic map* (1D PWLCM) defined by the formula:

$$F(x,p) = \begin{cases} x/p, & x \in [0,\ p), \\ (x-p)/(0.5-p), & x \in [p,\ 0.5), \\ (1-x-p)/(0.5-p), & x \in [0.5,\ 1-p), \\ (1-x)/p, & x \in [1-p,\ 1], \end{cases} \tag{4.1}$$

where $p \in (0,\ 0.5)$ (see Fig. 1). The map is simple (easy to compute) and is chaotic in the whole range of parameter p changes [12].

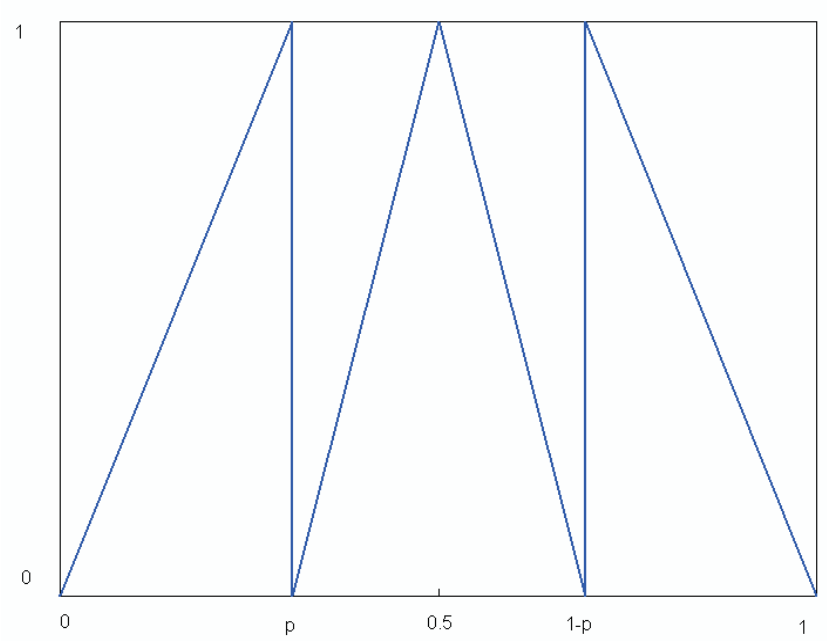

Fig. 1. 1D piece-wise linear chaotic map, defined by Eq. (4.1).

In order to avoid effects of dynamical degradation, we use a perturbation algorithm [12], defined by the formula:

$$x_{i+1} = rem\left(\mathbf{F}\left(x_i\right) + r_i,\ 1\right), \tag{4.2}$$

where $\mathbf{F}\colon [0,\ 1] \to [0,\ 1]$ is a given chaotic map, $r_i \in (0,\ 1)$ – i-th pseudorandom number from the generator with uniform distribution (PRNG), which perturbs the map, and $rem(\cdot,\ 1)$ means taking rest from division by 1 (taking the fractional part). The state of generator is determined by a number s (generator seed). With this map, conversion to floating-point numbers is done by simple division by 255, while returning to colors is done by multiplication by 255 and rounding to the nearest integer. Conversion does not make problems with decryption, because it is done always before and after making n iterations on the map. Therefore, it costs more computations. All the other operations are performed in group $\mathbf{Z}_{256}$ and the normalization process has an obvious nature of adding or subtracting 256. The key of the cipher is a pair $(p,\ s)$, i.e., the map control parameter p and the seed s of the pseudorandom number generator.

Encryption and decryption procedures are described below.

Algorithm 3. Improved CML cipher encryption procedure.	
Input:	s – seed, part of a cipher key
	j – number of cycles
	m – number of pixels
	IMG – stream of image pixels
	n – number of iterations
	M – chaotic map
	p – control parameter, part of a cipher key
	$RAND$ – stream of pseudorandom numbers from PRNG
Output:	stream of encrypted pixels
1.	initialize pseudorandom number generator with seed s
2.	**for** $i \leftarrow 1$ **to** $j \cdot m$ **do** $RAND(i) \leftarrow$ *next number from PRNG*
3.	**for** $cycle \leftarrow 1$ **to** j **do** steps from 4 to 10
4.	**for** $pixel \leftarrow 1$ **to** m **do** steps from 5 to 10
5.	$x_0 \leftarrow \dfrac{IMG(pixel\ -1)}{255}$
6.	**for** $i \leftarrow 1$ **to** n **do** $x_i \leftarrow M(x_{i-1}, p)$
7.	$k = m \cdot (cycle\ -1) +\ pixel$
8.	$x_n \leftarrow (x_n +\ RAND(k)) \bmod 1$
9.	$IMG(pixel) \leftarrow IMG(pixel) +\ round(x_n \cdot 255)$
10.	**if** $IMG(pixel) > 255$ **do** $IMG(pixel) \leftarrow IMG(pixel) - 256$

Algorithm 4. Improved CML cipher decryption procedure.

Input: s – seed, part of a cipher key
j – number of cycles
m – number of pixels
IMG – stream of encrypted image pixels
n – number of iterations
M – chaotic map
p – control parameter, part of a cipher key
$RAND$ – stream of pseudorandom numbers from PRNG

Output: stream of decrypted pixels

1. initialize pseudorandom number generator with seed s
2. **for** $i \leftarrow 1$ **to** $j \cdot m$ **do** $RAND(i) \leftarrow$ *next number from PRNG*
3. **for** $cycle \leftarrow j$ **to** 1 **do** steps from 4 to 10
4. **for** $pixel \leftarrow m$ **to** 1 **do** steps from 5 to 10
5. $x_0 \leftarrow \dfrac{IMG(pixel\ -1)}{255}$
6. **for** $i \leftarrow 1$ **to** n **do** $x_i \leftarrow M(x_{i-1}, p)$
7. $k = m \cdot (cycle\ -1) +\ pixel$
8. $x_n \leftarrow (x_n +\ RAND(k)) \bmod 1$
9. $IMG(pixel) \leftarrow IMG(pixel) -\ round(x_n \cdot 255)$
10. **if** $IMG(pixel) < 0$ **do** $IMG(pixel) \leftarrow IMG(pixel) + 256$

In both algorithms, as a pixel preceding the first one, the last image pixel is taken. Parameter k is used for indexing the stream from PRNG. As we can see, in the decryption procedure the numbers from generator are used in reverse order. Other operations were described above.

5. Implementation and security analysis

The improved version of the CML algorithm, presented above, was implemented in Matlab language to study its practical functioning. In our implementation p is a double precision floating-point number and s is an unsigned integer, both 64-bits. Entropy measurement and symmetry of the map [24] cause that the bit count of p is effectively equal to 53. Thus the size of the key-space is about $2^{53} \times 2^{64} = 2^{117}$, which is quite good for some applications.

The tests were done for an image of the size 256×256. The ciphertext turned out to be illegible even after a small number of iterations (e.g. $n = 5$), although it was checked that the ciphertext is not sensitive to small changes in the key. Thus, the accepted values were $n = 25$ and $j = 5$. The used key was (0.12345, 123). The plain image, the encrypted image and their grayscale histograms are shown in Fig. 2.

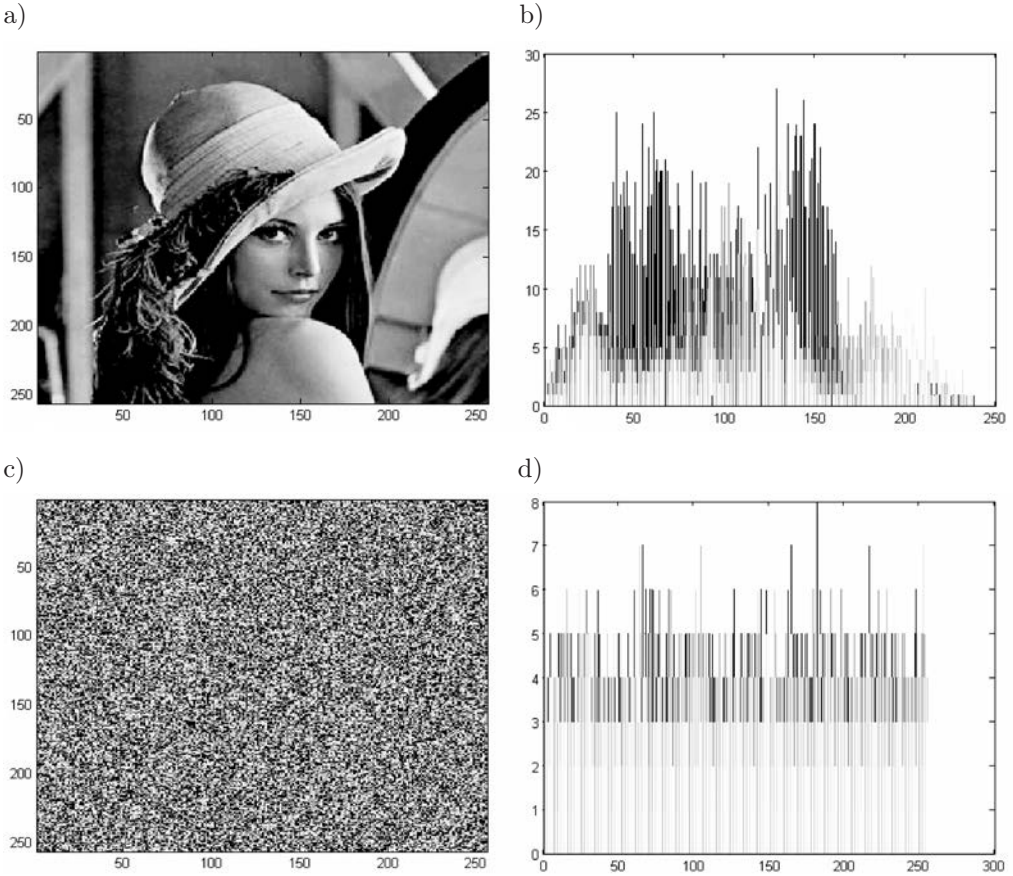

FIG. 2. Plain image (a), encrypted image (c) and their histograms (b and d).

As we can see, the encryption process is quite good with making histogram of grayscale values flat. It was checked that increasing iteration and cycle numbers do not provide significant improvement. In fact, histogram d) is not better than histogram made after only a few iterations and cycles. A situation with pixel's correlation is similar, see Fig. 3.

Tests of the sensitivity on a key change was carried out with parameters $n = 25$, $j = 5$. Firstly, the $(0.222,\ 2)$ key was used, then $(0.222 - 2^{-53},\ 2)$. Next, we took the first part of the key as constant and changed the other. First, the key was $(0.222,\ 123456789)$, then $(0.222,\ 123456788)$. Results of the subtraction of the encrypted image pairs are shown in Fig. 4.

The obtained ciphertexts in the a) case are identical only in 0.36%, whereas in case b) only in 0.41%. In the next test we encrypted the image with the key $(0.222,\ 2)$ and decrypted with the key $(0.222 - 2^{-53},\ 2)$. The other pair of keys was investigated analogously. The results are shown in Fig. 5.

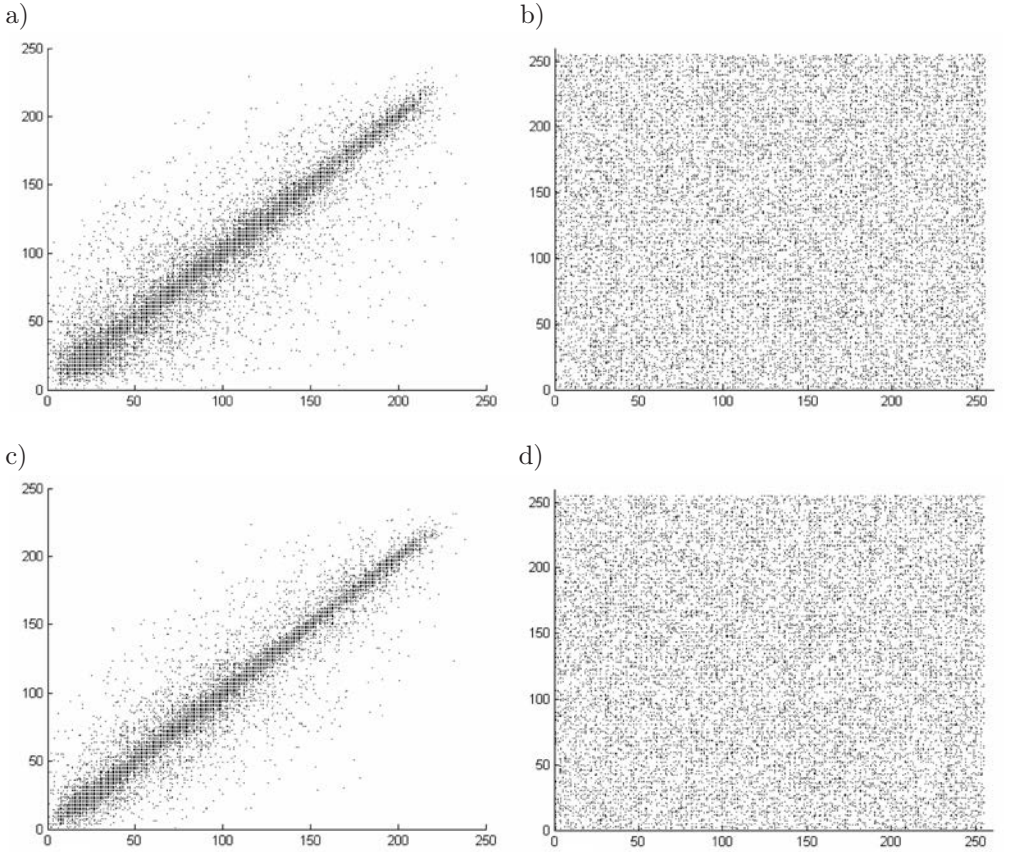

FIG. 3. Correlation between the neighboring pixels of plain image and encrypted image: horizontally (a and b), vertically (c and d).

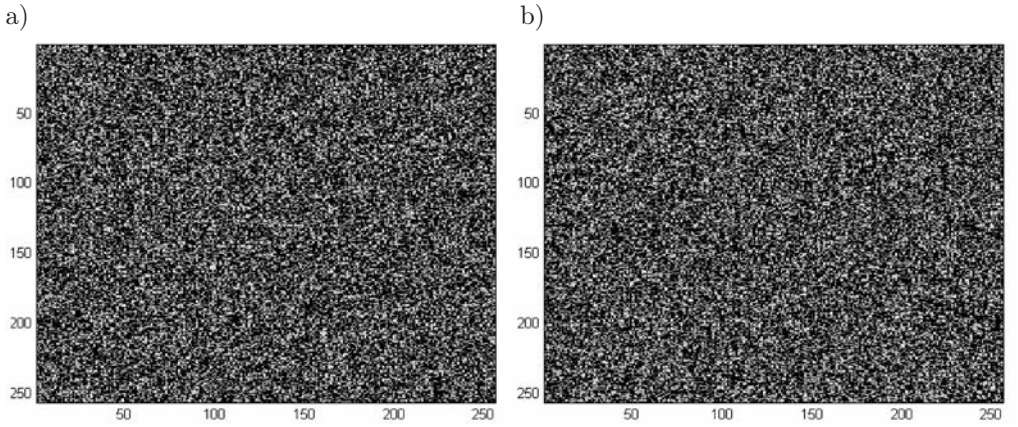

FIG. 4. Result of subtracting the images encrypted with the keys: a) $(0.222,\ 2)$ and $\big(0.222 - 2^{-53},\ 2\big)$; b) $(0.222,\ 123456789)$ and $(0.222,\ 123456788)$.

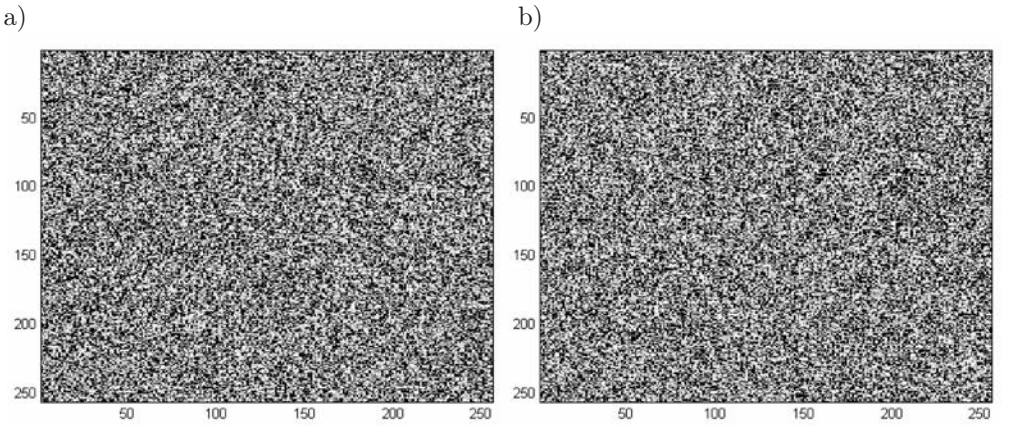

FIG. 5. Result of decryption an encrypted image using another key: a) encryption using $(0.222,\ 2)$, decryption using $(0.222 - 2^{-53},\ 2)$; b) encryption using $(0.222,\ 123456789)$, decryption using $(0.222,\ 123456788)$.

For the tests of sensitivity on small plain image changes, we used an image created by making black a square of 2×2 pixels of the original image. We used the key equal to $(0.222,\ 2)$, $n = 25$ iterations, $j = 5$ cycles. The result of subtracting of both images is presented in Fig. 6.

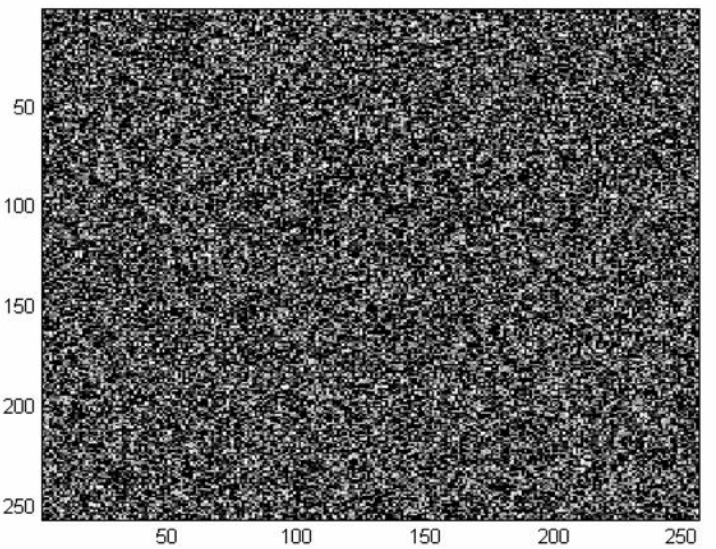

FIG. 6. Result of subtracting of two ciphertexts, obtained form very similar images and the same key.

The obtained ciphertexts are identical only in 0.39%. Thus, the cipher is sensitive to small changes in the plain image.

As it was mentioned, the proposed cipher's nature is similar to CBC encryption mode. We think that this property makes the chosen-plaintext attack difficult. Using chaos should prevent the cipher from the known-plaintext and ciphertext-only attacks.

6. Conclusions and future work

In this paper, we have presented several improvements of the errors found in the CML algorithm [21]. Our improved version of the cryptosystem is defined precisely, works properly and is ready for implementation. To work correctly, it does not have to make the data bigger by using floating point numbers to transmit the ciphertext. A comparison of both versions of the algorithm is presented in Table 4.

Table 4. Comparison of the two versions of the CML algorithm.

Feature	CML algorithm	New CML algorithm
key format	$\{a,\ n,\ j,\ m\}$ ={map control parameter, number of iterations, number of cycles, image size}	$\{p,\ s\}$ ={map control parameter, PRNG seed}
chaotic map used	logistic map	1D PWLCM Eq. (4.1)
dynamical degradation prevention	–	perturbation algorithm, defined by Eq. (4.2)
conversion to/from colors	twice: at the beginning and at the end; does not work properly	always before iterating map n times and after perturbation algorithm; works properly
normalization	by Eq. (2.2) and (2.3); does not work properly	by simple subtracting and adding 256; works properly
key length	using double precision numbers, 256×256 image and few more assumptions, about $2^{53} \times 2^5 \times 2^2 \times 2^8 \times 2^8 = 2^{76}$	about 2^{117}
ciphertext/ plaintext ratio	using floating point numbers as a ciphertext, $\frac{m \cdot 64 \text{ bits}}{m \cdot 8 \text{ bits}} = 8$	$\frac{m \cdot 8 \text{ bits}}{m \cdot 8 \text{ bits}} = 1$

Implementation made in Matlab language intensively increases the randomness of the image, even with small number of iterations. The pattern of the image is disappearing, the image looks like noise, histogram of grayscale values is flat and the correlation vanishes. The influence of the key and plain image to ciphertext is large, but the required number of iterations and cycles is bigger than the one required to obtain a ciphertext with a flat histogram. The size of the key-space in this implementation is about 2^{117}.

The proposed algorithm was tested with respect to its correctness, reversibility (in decryption device) and being ready for implementation. To test its effectiveness in professional applications, additional work should be carried out to write the adequate computer code in an optimal way. The required studies should include a choice of an appropriate PRNG in Algorithms 3 and 4.

References

1. C. E. Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal, **28**, 656–715, 1949.
2. Z. Kotulski, *Building block-ciphers: new possibilities*, Matematyka Stosowana, **4** (**45**), 1–24, 2003.
3. N. Masuda, G. Jakimoski, K. Aihara, L. Kocarev, *Chaotic block ciphers: from theory to practical algorithms*, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, **53**, 6, 1341–1352, 2006.
4. G. Alvarez, S. Li, *Some basic cryptographic requirements for chaos-based cryptosystems*, International Journal of Bifurcation and Chaos, **16**, (8), 2129–2151, 2006.
5. D.-I. Curiac, D. Iercan, O. Dranga, F. Dragan, O. Banias, *Chaos-Based Cryptography: End of the Road?*, Proc. IEEE Int. Conf. Emerging Security Information, Systems and Technologies, 71–76, 2007.
6. T. Habutsu, Y. Nishio, I. Sasase, S. Mori, *A secret key cryptosystem by iterating chaotic map*, Proc. EUROCRYPT'91, LNCS **547**, 127–140, Springer, Berlin 1991.
7. E. Biham, *Cryptanalysis of the Chaotic-Map Cryptosystem Suggested at EUROCRYPT'91*, LNCS, **547**, 532, Springer, Berlin 1991.
8. Z. Kotulski, J. Szczepański, *Discrete chaotic cryptography*, Annalen der Physik, **509**, (5), 381–394, 1997.
9. M. S. Baptista, *Cryptography with chaos*, Physics Letter A, **240**, 1, 50–54, 1998.
10. Z. Kotulski, J. Szczepański, K. Górski, A. Paszkiewicz, A. Zugaj, *Application of discrete chaotic dynamical systems in cryptography – DCC method*, International Journal of Bifurcation and Chaos, **9**, 6, 1121–1135, 1999.
11. E. Alvarez, A. Fernandez, P. Garcia, J. Jimenez, and A. Marcano, *New approach to chaotic encryption*, Physics Letter A, **263**, 4–6, 373–375, 1999.
12. S. Li, *Analyses and New Designs of Digital Chaotic Ciphers*, PhD thesis, http://www.hooklee.com/Thesis/ethesis.zip, 2005.
13. S. Li, G. Chen, X. Zheng, *Chaos-Based Encryption for Digital Images and Videos*, [in:] Multimedia Security Handbook, [Eds.] B. Furht and D. Kirovski 133–167, CRC Press, Boca Raton 2004.
14. Y. Mao, G. Chen, *Chaos Based Image Encryption*, [in:] Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neural Computing and Robotics, edited by E. Bayro-Corrochano, Springer, New York 2003.

15. A. Said, W. A. Pearlman, *A new fast and efficient image codec based on set partitioning in hierarchical Trees*, IEEE Trans Circuits and Systems for Video Technology, **6**, 6, 243–250, 1996.

16. J.-C. Yen, J.-I. Guo, *A new chaotic key-based design for image encryption and decryption*, Proc. IEEE Int. Conf. Circuits and Systems, **4**, 49–52, 2000.

17. J.-C. Yen, J.-I. Guo, *A new image encryption algorithm and its VLSI architecture*, [in:] Proc. IEEE Workshop Signal Processing Systems, 430–437, 1999.

18. Y. Mao, G. Chen, S. Lian, *A novel fast image encryption scheme based on 3D chaotic baker maps*, International Journal of Bifurcation and Chaos, **14**, 10, 3613–3624, 2004.

19. S. Li, X. Zheng, X. Mou, Y. Cai, *Chaotic encryption scheme for real-time digital video*, Proc SPIE on Electronic Imaging, San Jose CA USA, Real-Time Imaging VI, **4666**, 149–160, 2002.

20. J. Fridrich, *Symmetric ciphers based on two-dimensional chaotic maps*, International Journal of Bifurcation and Chaos, **8**, 1259–1284, 1998.

21. P. Pisarchik, N. J. Flores–Carmona, M. Carpio–Valadez, *Encryption and decryption of images with chaotic map lattices*, Chaos, **16**, 033118, 2006.

22. M. Dworkin, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, NIST Special Publication 800-38 A, http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf, 2001.

23. E. Ott, *Chaos in dynamical systems*, Cambridge University Press, London 1993.

24. A. Skrobek, P. Sukiennik, *Cryptanalysis of Chaotic Product Cipher*, [in:] Advances in Information Processing and Protection, [Eds.] J. Pejaś and K. Saeed 281–290 Springer, New York 2007.

25. K. Jastrzębski, *Cryptanalysis of some chaos-based algorithm of an image encryption*, MSc Thesis, supervisor: Z. Kotulski, Warsaw University of Technology, September 2007.

Received February 16, 2009; revised version September 17, 2009.

ENGINEERING TRANSACTIONS • *Engng. Trans.* • **57**, 2, 105–112, 2009
Polish Academy of Sciences • Institute of Fundamental Technological Research

MULTI-GOAL OPTIMIZATION OF A CARRY-MOULD

B. Reggiani [1)], F. Cosmi [2)]

[1)] **University of Bologna**
Department of Mechanical Engineering
Viale Risorgimento 2, 40136 Bologna, Italy

[2)] **University of Trieste**
Department of Mechanical Engineering
Via A. Valerio 10, 34127 Trieste, Italy

A common engineering task is the optimization of components that are part of multi-body assemblies, in which it is difficult to extrapolate and define the boundary conditions to be applied for the component optimization. This work presents a procedure for multi-goal optimization of components that are integrated in multipart engineering systems. The efficiency of the procedure is illustrated by means of a test case, a carry-mould that is part of a multi-component blowing machinery. Target goals of the optimization process are the minimization of moment of inertia and of global mass and the maximum allowable displacement in a number of control points.

Key words: design, multi-goal optimization, carry-mould, blow-machinery assembly, FE modelling.

1. Introduction

The optimum design of mechanical components is the one that best meets all the requirements specified by engineers, resulting to be as effective as possible in terms of their performance and reliability. Due to different reasons, optimization is frequently a difficult task. For instance, in many real problems, attention must be directed not only to minimization of a single function but to optimization of more than one target goal, with simultaneous satisfaction of the predefined constraints placed on the design. Moreover, typical engineering systems are described by a very large number of variables which even the most skilled designers are unable to take simultaneously into account without proper powerful numerical simulation tools. Besides, mechanical components are often a part of complex assemblies, thus making it difficult to extrapolate and define the boundary conditions to be applied in the component for its design optimization.

A procedure for investigation of the multi-goal optimum design of components that are integrated in complex engineering systems is presented in this work.

A carry-mould that is a part of the blowing machinery composed of several components, is used as a test component in order to illustrate the procedure. Target goals of the optimization are the minimization of moment of inertia and global mass of the carry-mould, while the main displacement in a number of control points is imposed to remain under an allowable peak value. Numerical scales and values have been excluded from the results because of confidentiality issues, but this does not affect comprehensibility and relevance of the results.

2. Optimization of the carry-mould

The original design of the carry-mould used as a test case to illustrate the proposed procedure is shown in Fig. 1a (base model). Two additional initial parametric geometries of the carry-mould were generated for a computationally efficient investigation of a number of potential designs: the mono-rib model (Fig. 1b) and the two-ribs model (Fig. 1c).

a) b) c)

Fig. 1. The initial parametric geometries of the carry-mould: a) the base model, b) the mono-rib model, c) the two-ribs model.

Parameterization of the base model involved the geometric variables that define the external profile of the carry-mould, the width and clearance angles of the rib and ribbings and the thickness around the upper hole. In addition, in the two-ribs and mono-rib models, also two lightening holes were parameterized in position and diameter. A limited number of geometric fixed constraints was imposed in the parameterization (location and diameter of the holes for the pins and position of the contact plate of the carry-mould).

The proposed optimization procedure allows to investigate the design space by the definition of a 3D FE (Finite Element) equivalent single-body model of the component, obtained as explained in the following.

First, a simplified 2D FE model of the blowing machinery was generated from the original 3D CAD model (Fig. 2a). Indeed, evaluation of numerical robustness and accuracy in complex 3D problems is extremely time-consuming and the 2D simplified model allows to identify (with smaller computational requirements) the average element dimension, the most critical contact regions and the proper solution parameters to be used in the component 3D FE model that will constitute the starting point for optimization. The 2D FE model of the assembly was generated by virtually cutting the 3D CAD model along the middle longitudinal cross-section (Fig. 2b) and by using the contour lines of components (Fig. 2c). Boundary conditions applied to the 2D model were analogous to those imposed on the 3D FE model but, in order to replicate the real 3D problem behaviour, the 2D model was also stiffened by constraining appropriate zones of the frame and by adding 2D beam elements with infinite stiffness where appropriate.

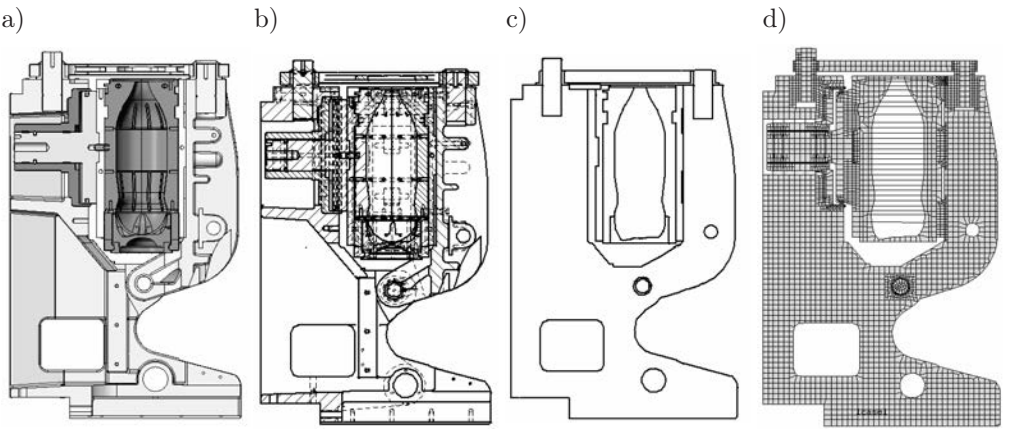

FIG. 2. a) Original 3D CAD model; b) 2D CAD model; c) simplified 2D CAD model; d) optimal 2D FE model.

A 3D FE model of the complete multi-body assembly (24 components) was successively generated in order to identify the values of displacements and contact pressures acting on the carry-mould and constituting the constraints for the successive optimization simulations. The meshed model had 171955 20-nodes tetrahedral elements and 235194 nodes. Boundary conditions applied to the model considered the blowing pressure, a vertical pushing force and the gripping screw forces acting in the real physical system.

Finally, the boundary conditions (displacements and contact pressure) derived by the 3D FE model of the assembly were imposed on the equivalent

single-body model of the carry-mould, by means of a set of purposely created grids of areas and points (Fig. 3).

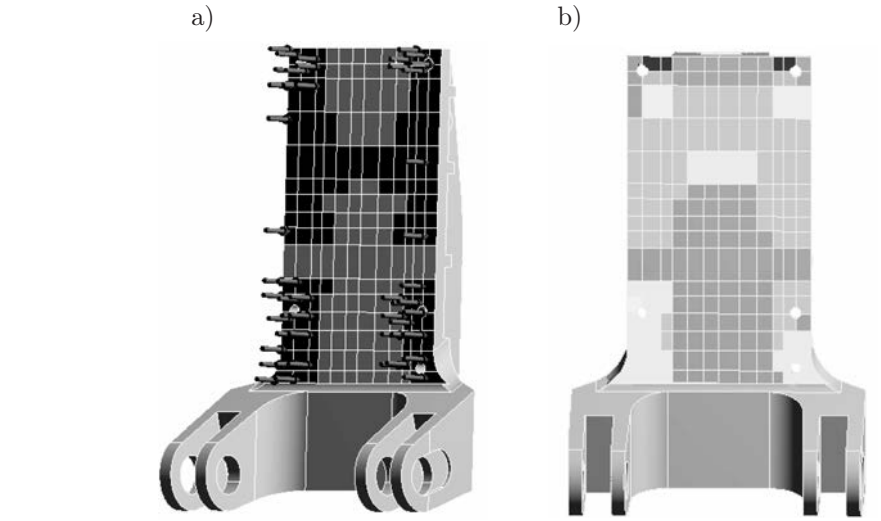

Fig. 3. Qualitative maps of the displacements (a) and contact pressure (b) applied on the carry-mould from the assembly 3D FE model simulation.

ModeFRONTIER MDO (Multi Design Objective) tool [2] was used for the multi-goal optimization of the carry-mould.

By adopting the equivalent single-body model of the examined component [1], the same output values as those obtained from the complete multi-body assembly 3D FE model were found. At the same time, a drastic reduction of the optimization process computing-time was achieved, thus allowing for the evaluation of a very large number of design solutions. In fact, while each complete multi-body assembly 3D FE model simulation required approximately 20 hours, the equivalent single-body model simulation took only 5 minutes. Moreover, the definition of an equivalent single-body model simplified the identification of the entities needed for optimization: the *input variables*, parameterized in the model (that is the geometric variables previously defined for the base, two-ribs and mono-rib models), *the output parameters* that have to be optimized, and the optimization *constraints*. As already mentioned, the target goals were the minimization of moment of inertia and of global mass (output parameters) of the carry-mould. The optimization constraints were applied in a number of control points in the contact plate with the blow-mould shell, where the maximum allowable discrepancy from the values obtained by the 3D FE assembly model was limited to 10%. Results were expressed by a set of feasible non-dominated solutions, the Pareto optimal set (Pareto front). The evolutionary algorithm used to solve the test problem was the Non-dominated Sorting Genetic Algorithm (NSGA-II) implemented in

modeFRONTIER [3, 4]. An initial population of 20 configurations was set in the NSGA-II algorithm for each of the three analysed parametric geometries. Each initial population was identified by a pseudo-random SOBOL DOE sequence, thus reducing the clustering effect in the design space uniform sampling.

Lastly, robustness and stability of each candidate solution were investigated. Uncertainties in manufacturing errors, material properties and applied loads on the equivalent FE single-body model were investigated by means of the Multi-Objective Robust Design Optimization (MORDO) tool in modeFRONTIER. These variables were regarded as Gaussian distributions [5], characterized by a fixed standard deviation of 50 μm for the geometric parameters and a 10% variation of the nominal values for the grid contact pressure. Literature provided reference for uncertainties on the elastic modulus, the Poisson coefficient and the material density [6, 7]. A sensitivity analysis and a convergence test of the target goals standard deviation were performed to establish the number of runs in the robust design routine. The configuration characterized by the lowest standard deviation of the objective functions was then chosen as the final optimum design.

3. Results

From the optimal 2D FE model of the assembly (Fig. 4) it followed that the most critical contact regions, requiring a smaller average elements dimension, were those including upper pins, probably because they were the most responsible for the model kinematics behaviour.

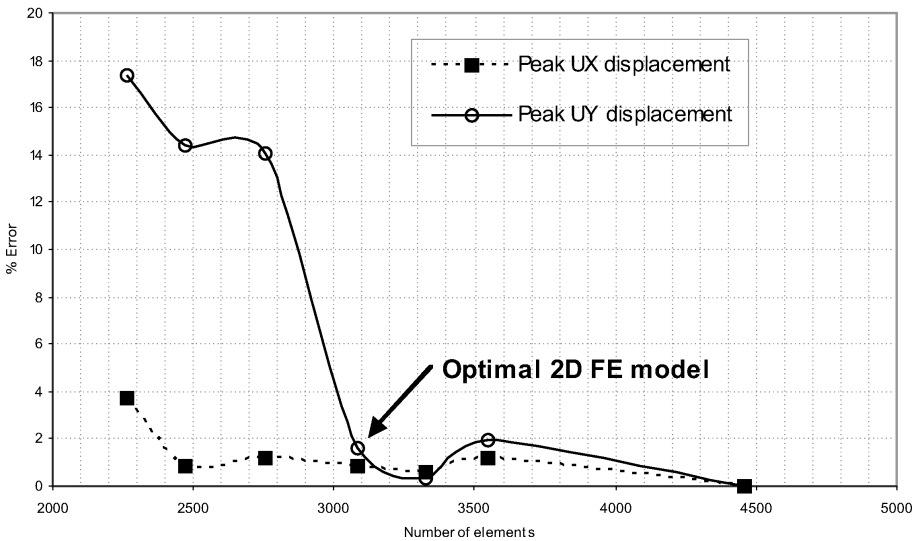

Fig. 4. Percentage error in output displacements with respect to the most refined FE model (assumed as the exact solution) vs the number of elements in the 2D FE model.

The results found for the optimal 2D FE model were used to set the average elements dimension in the 3D FE model of the assembly. A qualitative example of the results predicted by the 3D FE assembly model is shown in Fig. 5.

FIG. 5. Qualitative map of Von Mises stress distribution as predicted by the 3D FE model.

The good agreement between the single-body and the 3D assembly FE models outputs is qualitatively shown in Fig. 6.

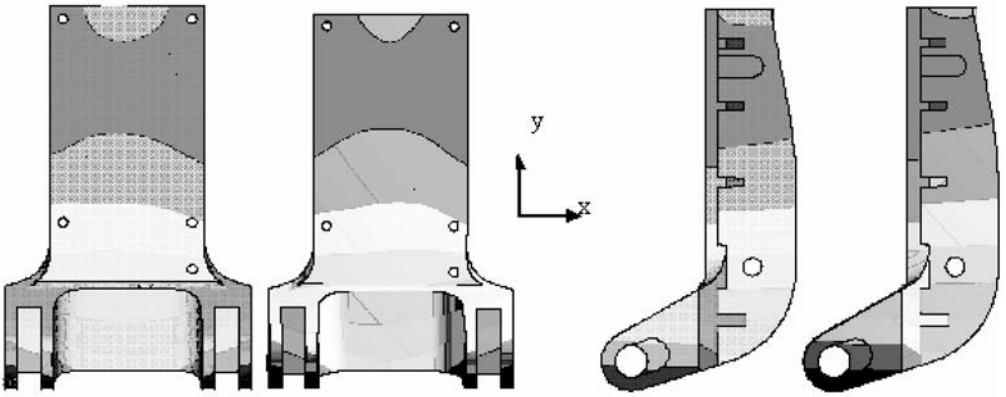

FIG. 6. Comparison of the map of the displacements along the x direction in the 3D FE model (right) and in the single-body model (left) (front and lateral view).

The displacements in a selected set of benchmark points, predicted by the equivalent single-body model, showed an average percentage error of 1.3±1% with respect to the analogous displacements computed by the 3D FE model of the assembly, indicating a very good agreement between the results.

The optimization procedure gave a total number of 6 solutions to be the candidates for the final optimum design (three for the base model, one for the

mono-rib model and two for the two-ribs model). For each original geometry, these solutions were the designs meeting the highest number of constraints on displacements, with the highest percentage improvement of the output objective functions (Table 1).

Table 1. Best target goals improvements achieved with candidate optimal designs.

Goal (minimization)	% Improvement		
	Base model	Mono-rib model	Two-ribs model
Mass	10.1	4.9	2.5
Moment of interia	11.4	8.3	5.7

Among these solutions, the design chosen as optimum was the one exhibiting the highest stability, in terms of objective functions, with respect to the uncertainties of the input parameters. Robust design analyses were preformed only for the base and two-ribs models, which produced more than one candidate solution.

Among these designs, the base-model candidate solutions were the most stable with respect to uncertainties of the input parameters, being characterized by a lower standard deviation. Thus, the final optimum design was chosen to be the geometric configuration of the base model that showed the highest percentage of improvement in terms of objective functions.

4. Conclusions

A novel procedure for the multi-goal design optimization of component part of complex assemblies was illustrated in this work by a test case. The opportunity to perform an extensive investigation in the optimum design space constitutes the principal benefit by adopting this procedure. In fact, by defining a 3D equivalent single-body model of the component, a drastic reduction of computation time is achieved without significant loss in the solution accuracy. The impact of uncontrollable variations of variables on design solutions could also be examined by means of the developed methodology. The efficient investigation of the optimization design space allowed to identify and choose the most robust and stable configuration as the final optimum design.

References

1. F. Cosmi, *A finite element method comparison of wear in two metal-on-metal total hip prostheses*, In the Proceedings of the I MECH E Part H Journal of Engineering in Medicine, **220**, 871–79, 2006.

2. www.esteco.com

3. O. Koksoy, *Robust design using Pareto-type optimization: A genetic algorithm with arithmetic crossover*, Computer & Industrial Engineering, **55**, 208–218, 2008.

4. F. Cosmi, *Ottimizzazione multiobiettivo di cambi di velocità per uso automobilistico: progettazione preliminare del gruppo ingranaggi-sincronizzatori-alberi* [in Italian], In Proceedings of the XXVIII AIAS Conference, Vicenza, Italy, 445–58, 1999.

5. C. Poloni, *Multi-objective robust design optimization of an engine crankshaft*, III European Conference on Computation Mechanics Solids, Structures and Coupled Problems in Engineering, Lisbon, Portugal, 2006.

6. UNI EN 1563, *Founding- Spheroidal graphite cast irons* [in Talian], 2004.

7. R.C. Juvinall, *Fundamental of Machine Component Design*, John Wiley & Sons Inc., 2005.

Received March 23, 2009.

ENGINEERING TRANSACTIONS • *Engng. Trans.* • **57**, 2, 113–123, 2009
Polish Academy of Sciences • Institute of Fundamental Technological Research

VARIATION OF MECHANICAL PARAMETERS OF ENGINEERING MATERIALS UNDER TENSION DUE TO CYCLIC DEFORMATION BY TORSION

Z. L. K o w a l e w s k i [1),2)], T. S z y m c z a k [2),3)]

[1)] **Institute of Fundamental Technological Research**
Polish Academy of Sciences
Pawińskiego 5B, 02-106 Warszawa, Poland

[2)] **Motor Transport Institute**
Jagiellońska 80, 03-301 Warszawa, Poland

[3)] **Białystok Technical University**
Faculty of Mechanical Engineering
Wiejska 45C, 15-351 Białystok, Poland

The paper presents experimental results of investigations carried out under complex stress state on the 2024 aluminium alloy (used by aircraft industry) and P91 steel (used at power plants). Second-order effects associated with cyclic loadings enforced by the trapezoidal signals in the two mutually perpendicular directions are identified. It is shown, how the cyclic loading and its parameters (strain amplitude and frequency) influence the simultaneous monotonic loading in the direction perpendicular with respect to the cyclic one. Moreover, the paper presents an analysis of the selected mechanical properties variations on the basis of an initial yield locus evolution.

1. Introduction

The influence of different forms of shear deformation of engineering materials on their mechanical parameters variation during parallel or subsequent loading processes has been investigated by many research groups, e.g. [1, 7, 9, 10, 12, 13]. The experimental results of these tests reflect a great role of the shear deformation connected with location and distribution of material grains [12], enforcing of slip lines direction [13] or identification of characteristic dislocation structures associated with cyclic loading, for a range of shear stress amplitudes. There is also a strong interest in experiments evaluating the influence of torsion cycles on the materials behaviour after prestraining due to monotonic deformation [6], or tension-compression cycles carried out up to the saturation state [2]. Looking at the available publications, a new trend in material testing can be observed in

the last decade. It is related to the cyclic loading application for a modification of some well-known forming processes [3–5]. Such an approach is important not only from the technological point of view, but also is essential for researchers developing new FEM codes and constitutive equations [8].

The paper presents the identification of material effects due to various combinations of cyclic and monotonic loadings.

2. Identification of cyclic loading influence on the material deformation in the perpendicular direction

2.1. A role of torsion cycles for cyclic deformation in axial direction of the 2024 aluminium alloy

All strain-controlled tests were carried out on the 2024 aluminium alloy under the biaxial stress state, being a combination of an axial force and twisting moment, both varying cyclically. The control signals were designed to form a square in the strain plane. It was achieved by the combination of two trapezoidal loading signals mutually delayed (when the first signal attained the maximum, then the second one started to increase linearly while the first one kept the constant value; when the second signal attained the maximum, the first one started to decrease up to the minimum while the second one kept the constant value, and so on). The main purpose of the programme was to identify second-order effects associated to the non-proportional cyclic loading along the square strain path.

An interesting feature can be easily noticed looking at the courses of stress and strain signals, Fig. 1a; 1b. A significant reduction of stress components magnitude takes place. It is visible when one of the control loading signals changes the direction (i.e. turns back). The second-order effects mentioned above are

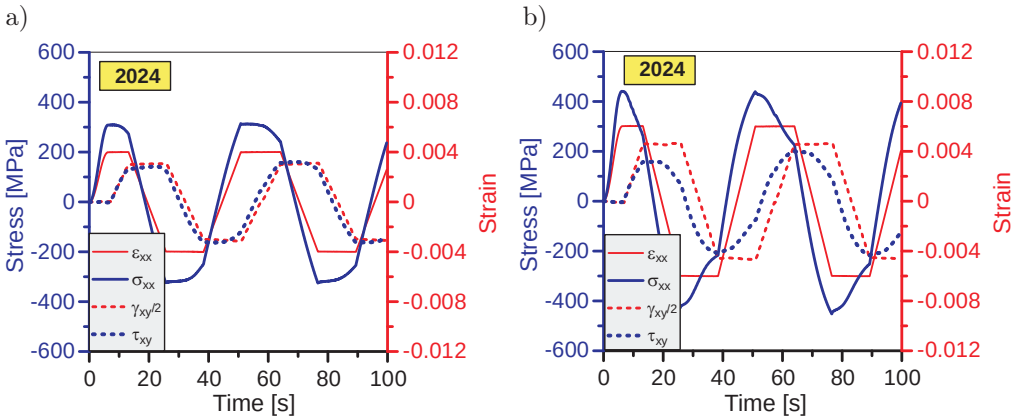

Fig. 1. Variations of the strain and stress signals due to cyclic loading realized along the square strain path. Effective strain amplitude: a) ±0.4%; b) ±0.6%.

especially considerable when the amount of strain amplitude increases. For example, in the case of the cyclic strain amplitude equal to ±0.4% a drop of the axial stress reaches about 100 MPa, whereas for ±0.6% it equals 250 MPa.

The influence of complex cyclic loadings acting along square strain path on the mechanical behaviour of the 2024 aluminium alloy can be evaluated on the basis of the data shown in Fig. 2, where the selected experimental results are presented. The results exhibit a hardening effect of the material. It is expressed by a gradual increase of stress amplitude and hysteresis loops. The effect increases with the strain amplitude increase. Moreover, the material does not reach the saturation state after the applied number of cycles. Both diagrams in Fig. 2 also well identify the axial stress reduction. Direct reason of that effect is connected with unloading in the torsion direction.

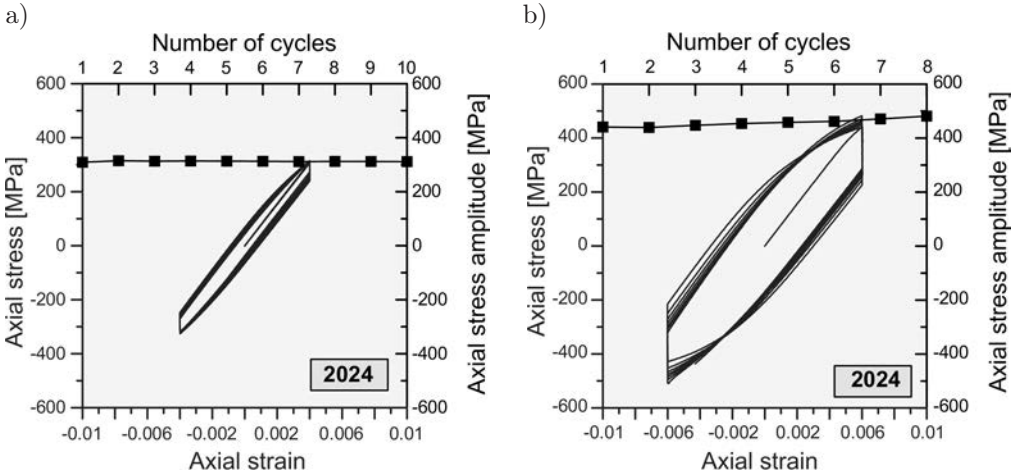

FIG. 2. Stress-strain variations and stress amplitude evolution due to the loading programmes shown in Fig. 1. Effective strain amplitude: a) ±0.4%; b) ±0.6%.

A rapid stress drops observed during cyclic loading along a square strain path was further investigated on the P91 steel, using the experimental programme in which torsion cycles were superimposed on monotonic tension. The representative experimental results of these tests are presented in the next point of this paper.

2.2. An influence of torsion-reverse-torsion cycles on uni-axial tension of the P91 steel

The experimental programme was carried out for a small value of the total strain, less than 1%. The main experimental objectives were focused on evaluation of:

- the influence of torsion-reverse-torsion cycles on the tensile characteristic and conventional mechanical parameters of engineering materials;
- the role of delayed torsion cycles on the behaviour of materials during the monotonic tension;
- an influence of the cyclic loading frequency on the tensile characteristics.

The P91 steel, commonly applied in the power industry, was investigated. A control parameter in the form of cyclic strain amplitude was designed to have a triangular shape and frequency equal to 0.5 Hz or 1 Hz.

All tests were carried out at room temperature using thin-walled tubular specimens with 1.5 mm wall thickness. The biaxial stress state was obtained using various combinations of axial force and twisting moment. All loading programmes were strain-controlled. The experimental programme contained selected combinations of monotonic and cyclic loadings, i.e. the torsion-reverse-torsion cycles were superimposed on the monotonic tension.

In the last part of the experimental programme, the subsequent yield surfaces for a plastic offset strain equal to 10^{-5} were determined. It enabled investigation of the initial yield surface evolution due to the loading history applied.

The representative loading programme is shown in Fig. 3. It presents some variations of the axial and shear strain components versus time. Stress responses in the programme are illustrated in Fig. 4. Variations of the axial stress express the material hardening in the direction of tension, while those for the shear stress observed identify a lack of any significant effects.

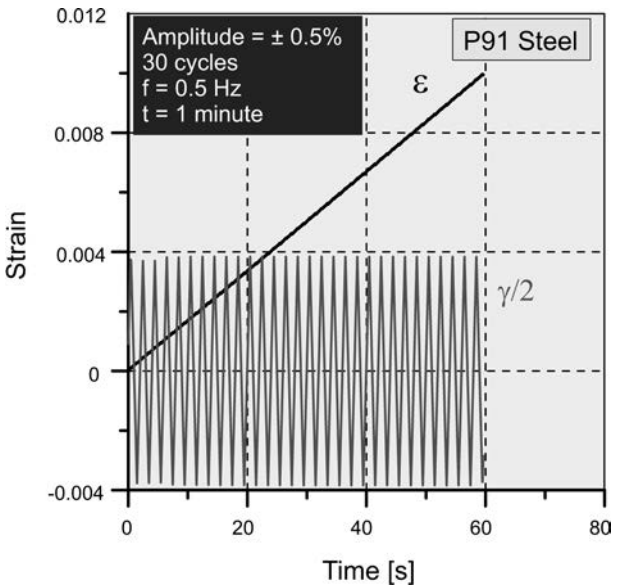

FIG. 3. Strain-controlled loading paths (ε – axial strain, $\gamma/2$ – shear strain).

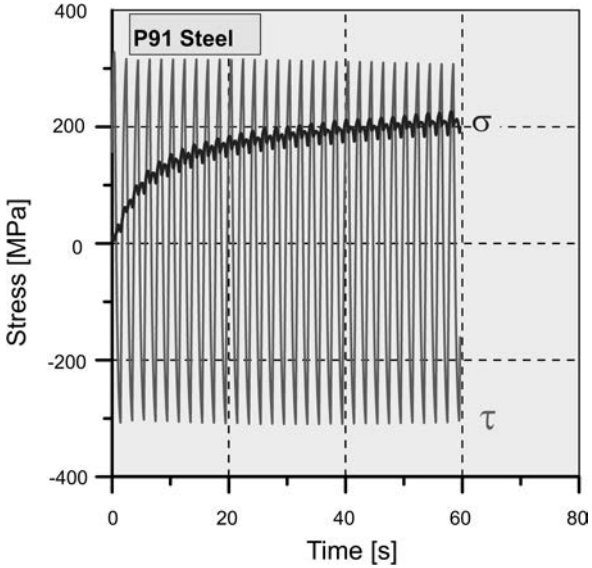

FIG. 4. Stress responses in the loading program shown in Fig. 3 (σ – axial stress, τ – shear stress).

In the first part of experiment, an influence of the cyclic strain amplitude on the basic mechanical parameters evolution was investigated. As it is shown in Fig. 5, the torsion-reverse-torsion cycles associated with monotonic tension

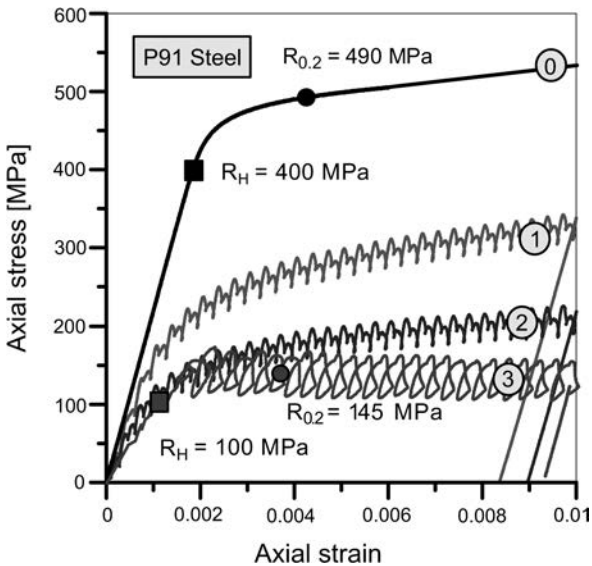

FIG. 5. Comparison of typical tensile characteristic (0) with tensile characteristics due to monotonic tension, superimposed on the torsion-reverse-torsion cycles for strain amplitude equal to: ±0.3% (1), ±0.5% (2), ±0.7% (3).

caused variations of the tensile characteristic. A significant decrease of the axial stress can be observed. An increase of the cyclic shear strain amplitude led to the further decrease of the stress-strain characteristic. As a consequence, due to the cyclic loading applied, the conventional mechanical parameters, such as the proportional limit and yield point, were significantly reduced. It is expressed by an essential drop of the yield point from 490 MPa to 145 MPa (Fig. 5).

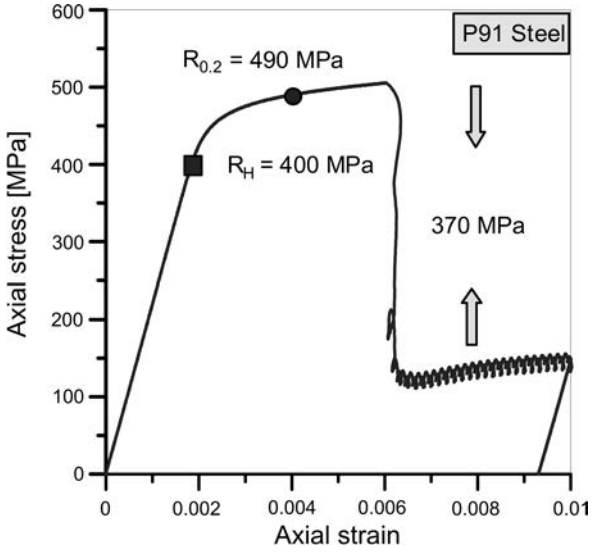

FIG. 6. Tensile characteristic of the P91 steel determined in assistance of torsion cycles (±0.5%), delayed with respect to monotonic axial loading.

The stress-strain diagrams showing the results of tests for the 2024 aluminium alloy identify a transient character of the axial stress reduction during tension associated with cyclic loading [9, 11]. This conclusion can be proved by determination of the yield surfaces for materials after standard tension tests and after the tension carried out in the presence of torsion cycles.

Thus, the next step of the experimental programme comprised the tests, the main aim of which was to check whether the axial stress reduction (as a consequence of the axial force lowering) during tension had a permanent character. The yield surface concept was applied. For each yield surface determined it was assumed that the total strain in the axial direction must be the same. The representative results for the P91 steel are presented in Fig. 7. As it is clearly seen, the subsequent yield surfaces for the material confirm that the axial stress reduction is related only to torsion cycles during monotonic tension. Looking at the magnitudes of tension stress achieved for the same offset strain, instead of reduction their increase can be observed. Therefore, it can be concluded that

the comparison of the subsequent yield loci with the initial yield surface exhibits only an influence of the loading history applied, and moreover, it proves a transient character of the axial force reduction, which can be solely attributed to cycles acting in the perpendicular direction.

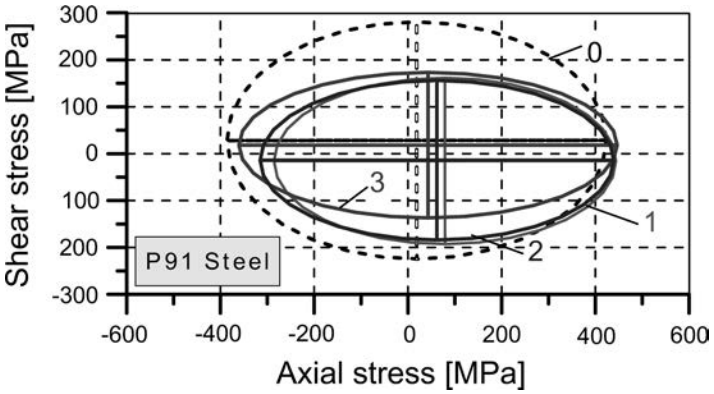

FIG. 7. Evolution of the initial yield surface (0) for the P91 steel due to torsion-reverse-torsion cycles for strain amplitude equal to: ±0.3% (1), ±0.5% (2), ±0.7% (3).

Taking into account the evolution of the initial yield surface origin, it is easy to see a reduction of the residual stresses in the torsion direction for the material subjected to the highest value of the torsion cyclic strain amplitude. In order to check whether a further increase of the cyclic strain amplitude may further eliminate the residual stresses from the material, additional tests were carried out. They were performed for two combinations of cyclic and monotonic loading having the same value of strain amplitude equal to ±0.8%, Fig. 8. At first, the material was subjected to monotonic torsion (up to 1% prestrain) assisted by tension-compression cycles and then, using another specimen, it was loaded monotonically by increasing axial force (leading to 1% prestrain) and by reversible twisting moment. In the next step, directly after termination of these loading programmes, the yield surfaces were determined. Their comparison with the initial yield locus confirms the transient character of a stress reduction observed on the monotonic loading direction when cycles were in progress. Also, a tendency to residual stresses reduction due to the increase of cyclic strain amplitude was approved. The results presented in Fig. 8 delivered an additional important knowledge on the material behaviour, namely, the P91 steel subjected to cyclic loading exhibits the softening effect observed on the directions corresponding to those of the cycles applied. Similar conclusions can be formulated on the basis of the results presented in Fig. 9. It shows a comparison of the initial yield locus with the subsequent yield surface determined after termination of the loading programme illustrated in Fig. 6. Despite the delay of cyclic

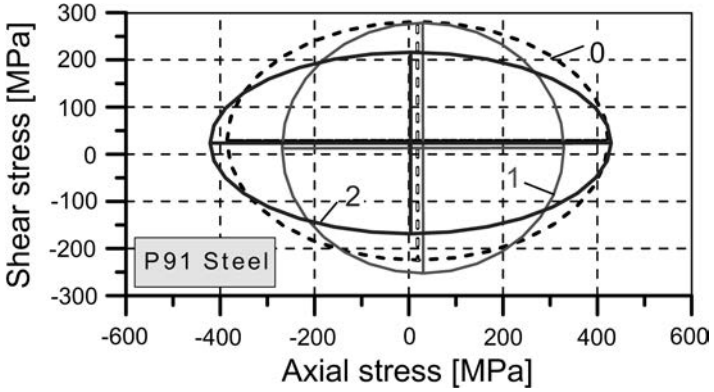

FIG. 8. Comparison of the initial yield surface (0) with the subsequent yield surfaces determined after monotonic torsion combined with tension-compression cycles (1) and after monotonic tension and by torsion cycles (2). For both cyclic loadings, the effective strain amplitude was equal to ±0.8%.

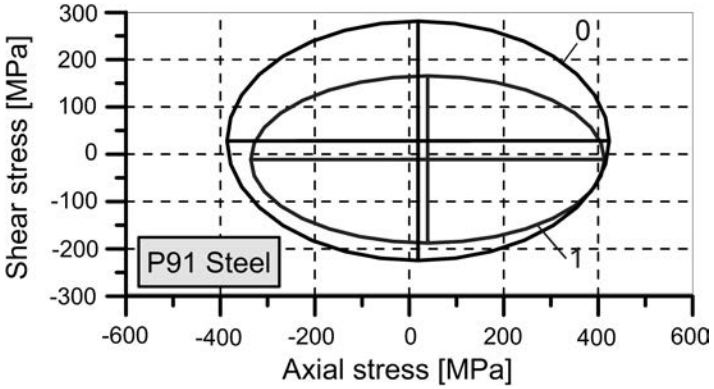

FIG. 9. Comparison of an initial yield surface (0) with a subsequent yield surface (1) after the test shown in Fig. 6.

torsion with respect to monotonic deformation due to tension, the same effects were obtained, i.e. softening of the steel in the directions of cyclic preloading and a lack of stress reduction observed during an acting of the torsion-reverse-torsion cycles.

The experimental programme also contained the tests evaluating the influence of the cyclic loading frequency on the tensile characteristics. As mentioned earlier, two values of the frequency were taken into account: 0.5 Hz and 1 Hz. The results are presented in Fig. 10.

As it is shown, only a small variation was achieved, and therefore further investigations in this matter are required. They should cover a much wider range of the frequency variation.

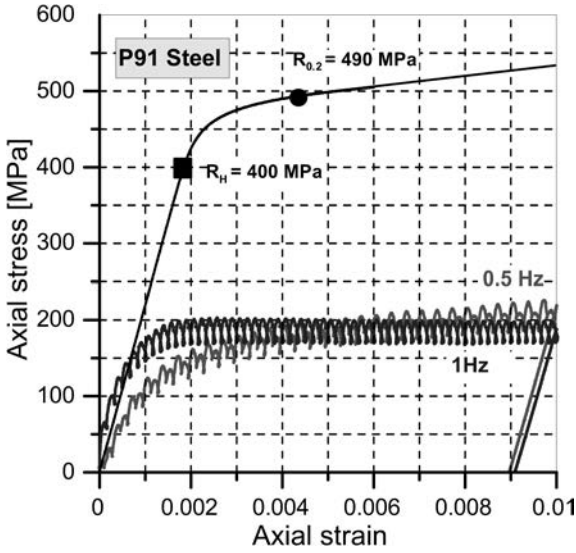

FIG. 10. Illustration of the effect of frequency variation on the tensile characteristics.

3. FINAL REMARKS

The effects presented in the paper are especially important for solid mechanics development, since they can be used to formulate new constitutive models. On the other hand, they provide an essential knowledge necessary for possible modification of some forming processes commonly applied in the industry.

The investigations carried out on the P91 steel and 2024 aluminium alloy allow to formulate the following conclusions and remarks:

- for the non-proportional cyclic loading along a square strain path, a significant reduction of stress components was identified. It was observed during each turn back of cyclic loading components;
- torsion-reverse-torsion cycles during monotonic tension cause a significant decrease of the proportional limit and yield point;
- an increase of the strain amplitude of torsion cycles improves material ductility in the tension direction;
- a reduction of the yield point and proportional limit increases with the cyclic strain amplitude increase;
- an axial stress reduction due to the presence of torsion cycles is not permanent, it vanishes after cyclic loading interruption;
- an initial yield surface evolution does not confirm rapid reduction of the selected mechanical parameters during tension assisted by cyclic torsion, it only points out their variations due to the loading history applied;

- the frequency variation of cyclic loading, within the range of values considered, caused only a little variation of the tensile characteristic.

References

1. A. Abdul–Latif, M. Chadli, *Modelling of the heteregenous damage evolution at the granular scale in polycrystals under complex cyclic loadings*, Int. J. Damage Mech., **16**, 133–158, 2007.
2. A. Benallal, D. Marquis, *An experimental investigation of cyclic hardening of 316 stainless steel under complex multiaxial loadings*, Trans. 9th SMIRT, 385–393, 1987.
3. W. Bochniak, A. Korbel, *KOBO Type Forming: forging of metals under complex conditions of the process*, J. Mat. Proc. Tech., **134**, 1, 120–134, 2003.
4. W. Bochniak, A. Korbel, R. Szyndler, R. Hanarz, F. Stalony–Dobrzański, L. Błaż, P. Snarski, *New forging method of bevel gears from structural steel*, J. Mater. Proc. Tech., **173**, 75–83, 2006.
5. W. Bochniak, A. Korbel, R. Szyndler, *Innovative solutions for metal forming*, Proc. Inter. Conf. MEFORM 2001 – Herstellung von Rohren und Profilen, Institut für Metallformung Tagungsband, 239, Freiberg/Riesa, 2001.
6. W. P. Jia, J. V. Fernandes, *Mechanical behaviour and the evolution of the dislocation structure of copper polycrystal deformed under fatigue-tension and tension-fatigue sequential strain paths*, Mater. Sci. Eng., **A348**, 133–144, 2003.
7. Jixi Zhang, Yanyao Jiang, *An experimental study of the formation of typical dislocation patterns in polycrystalline copper under cyclic shear*, Acta Materialia, **55**, 1831–1842, 2007.
8. L. X. Kong, P. D. Hodgson, *Constitutive modelling of extrusion of lead with cyclic torsion*, Mater. Sci. Eng., **A 276**, 32–38, 2000.
9. Z. L. Kowalewski, T. Szymczak, *Effects observed in engineering materials subjected to monotonic and cyclic loading due to tension-torsion combinations*, PLASTICITY '09, 15th International Symposium on Plasticity & Its Current applications, St. Thomas, Virgin Islands, USA, Jan. 3–8 2009, 196–198, 2009.
10. Z. L. Kowalewski, T. Szymczak, *A role of cyclic loading at modification of simple deformation processes of metallic materials*, The 5th International Symposium on Failure Mechanics of Materials and Structures, Augustów, 3–6 June 2009, Poland, 59–60, 2009.
11. Z. L. Kowalewski, T. Szymczak, *Effect of cyclic loading due to torsion on the monotonic tension parameters of engineering materials*, International Symposium on Plasticity 2007 and its current applications: PLASTICITY'07: 13th International Symposium, Girwood, Alaska, June 2–6, 2007, USA, 181–183, 2007.
12. A. Kumar, S. K. Samanta, K. Mallick, *Study of the effect of deformation on the axes of anisotropy*, J. Eng. Mat. Tech., **113**, 187–191, 1991.
13. R. Mnif, M. Kchaou, R. Elleuch, F. Halouani, *Cyclic behavior and damage analysis of brass under cyclic torsional loading*, J. Fail. Anal. and Preven., 450–455, 2007.

Received July 6, 2009; revised version October 13, 2009.

ENGINEERING TRANSACTIONS **Appears since 1952**

Aims and Scope

ENGINEERING TRANSACTIONS promotes research and practise in engineering science and provides a forum for interdisciplinary publications combining mechanics with material science, electronics (mechanotronics), medical science and biotechnologies (biomechanics), environmental science, photonics, information technologies and other engineering applications. The Journal publishes original papers covering a broad area of research activities including experimental and hybrid techniques as well as analytical and numerical approaches. Engineering Transactions is a quarterly issued journal for researchers in academic and industrial communities.

Address of the Editorial Office:
Engineering Transactions
Institute of Fundamental Technological Research
Pawińskiego 5B,
PL 02-106 Warsaw, Poland

Phone: (48-22) 826 60 22, Fax: (48-22) 826 98 15, E-mail: publikac@ippt.gov.pl

Abstracted/indexed in:

Applied Mechanics Reviews, Current Mathematical Publications, Inspec, Mathematical Reviews, MathSci, Zentralblatt für Mathematik.

`http://et.ippt.gov.pl/`

SUBSCRIPTIONS

Address of the Editorial Office: Engineering Transactions
Institute of Fundamental Technological Research
Pawińskiego 5B, PL 02-106 Warsaw, Poland
Tel.: (48-22) 826 60 22, Fax: (48-22) 826 98 15, E-mail: publikac@ippt.gov.pl

Subscription orders for all journals edited by IPPT (Institute of Fundamental Technical Research) may be sent directly to the Publisher: Institute of Fundamental Technological Research
e-mail: subscribe@ippt.gov.pl

Please transfer the subscription fee to our bank account: Payee: IPPT PAN,
Bank: Pekao S.A. IV O/Warszawa,
Account number 05124010531111000004426875.

All journals edited by IPPT are available also through:

- Foreign Trade Enterprise ARS POLONA ul. Obrońców 25,
  03-933 Warszawa, Poland, Tel. (48-22) 509 86 38, 509 86 37
  e-mail: arspolona@arspolona.com.pl
- RUCH S.A. ul. Jana Kazimierza 31/33,
  01-248 Warszawa, Poland,
  Tel. (48-22) 532 88 16, Fax (48-22) 532 87 31
  e-mail: prenumerata@okdp.ruch.com.pl
- International Publishing Service Sp. z o.o ul. Noakowskiego 10 lok. 38
  00-664 Warszawa, Poland, Tel./fax: (48-22) 625 16 53, 625 49 55
  e-mail: books@ips.com.pl

Warunki prenumeraty

Prenumeratę na wszystkie czasopisma wydawane przez IPPT PAN przyjmuje Dział Wydawnictw IPPT. Bieżące numery można nabywać, a także zaprenumerować roczne wydanie Engineering Transactions, bezpośrednio w IPPT PAN,
ul. Pawińskiego 5B, 02-106 Warszawa
Tel.: (48-22) 826 60 22; Fax: (48-22) 826 98 15
e-mail: subscribe@ippt.gov.pl

Czasopisma można zamówić (przesyłka za zaliczeniem pocztowym) w Warszawskiej Drukarni Naukowej PAN, ul. Śniadeckich 8, 00-656 Warszawa
Tel./Fax (48-22) 628 87 77; (48-22) 628 76 14, e-mail: dystrybucja@wdnpan.pl
Wpłaty na prenumeratę przyjmują także regionalne Działy Sprzedaży Prasy RUCH S.A.
Infolinia: 804 200 600. Zamówienia można przesyłać pocztą elektroniczną ze strony www.prenumerata.ruch.com.pl

Arkuszy wydawniczych 4.5; Arkuszy drukarskich 3.5
Papier offset. kl. III 70 g. B1
Oddano do druku w listopadzie 2009 r. Druk ukończono w grudniu 2009 r.
Skład w systemie LaTeX K. Jezierska
Druk i oprawa: Drukarnia Braci Grodzickich, Piaseczno ul. Geodetów 47A