UDC 621.327

THE MODEL OF AVALANCHE — RELATING EFFECT IN THE PROCESS OF IMAGES RECONSTRUCTION IN THE COMBINED CRYPTOSEMANTIC SYSTEMS ON THE BASE OF POLYADYC PRESENTATION

Barannik V. V., Dr. Sci. (Eng.), Prof.; Sydchenko S. A., PhD; Larin V. V., PhD

The Kharkov university of Air Forces of I. Kozheduba

kszi@ukr.net

Розглянуто основні етапи побудови методології скриття семантичної структури зображень у стійких системах на базі двовимірного поліадичного уявлення в результаті декодування по помилково підібраних підставах елементів ДПЧ, що базується на: формуванні системи службових даних на базі динамічних діапазонів елементів ДПЧ; моделі лавино-зв'язувального ефекту в процесі реконструкції зображень у комбінованих криптосемантичних системах на базі поліадичного уявлення.

Ключові слова: лавино-зв'язувальний ефект, реконструкція, поліадичне представлення, криптосемантичні системи, декодування.

The basic stages of methodology hiding construction of semantic structure of images are expounded in decoded proof systems on the base of 2-D polyadic presentation as a result of decoding on the by mistake neat grounds of DPN elements, being based on: forming of the official information system on the base of dynamic ranges of DPN elements; models of avalanche relating effect in the process of images reconstruction in combined crypto semantic systems on a base poliadic presentations.

Key words: avalanche-relate effect, reconstruction, polyadyc presentation, cryptosemantic systems, decoding.

Introduction

In the modern systems the questions related to treatment and information transfer run into the traditional necessity of diminishing providing of transferrable information volumes with the set level of confidentiality. However for the last decade the volume of video information traffic was sharply multiplied [1; 2]. The directions in the control systems, related to the receipt of information transferrable by the images, develop. Consequently ***there*** is ***the*** actual ***scientifically - applied task*** conditioned by the necessity of providing of semantics defense of images.

It is in — process [3; 4] offered directions of providing of the decoded firmness of images on the base of the compression systems. In this case the special interest causes approach in relation to creation of the combined cryptosemantic transformations in the systems of polyadyc presentation. A necessity to estimate possibility of the official part use as key one in the process of organization cryptosemantic systems on the base of polyadyc presentation appears therefore. Means ***the purpose*** of researches consists in construction of origin model and errors propagation in the process of polyadyc codes constructions decoding.

The basic material

In the conditions of the combined decoded — proof presentation (DPP) construction of images an important place is taken to forming of official constituent of codes constructions. It is explained by the necessity of change providing of standard process of compression and hiding of semantic and structural maintenance of the processed images. For these purpose components of official constituent: from one side participate in the process of organization of compression on key information; from other side is exposed to the cryptographic decipherment in the systems of compression with next action.

In the case of the combined system organization of DPP on the basis of compression polyadyc codes official information appear on the base of dynamic ranges of elements. It provides:

а) creations of condition for meaningful influence of official information on the process of codegram forming of informative part;

б) that official information characterize maintenance of the concrete processed local fragment of image. This property is based on that a dynamic range is concrete description of the processed fragment of images, and depends on his semantic maintenance.

In the conditions of combined DPP construction on the base of the compression system an important place is taken to the necessity of compression organization on key information. In the case of DPP construction on the base of the polyadyc encoding systems it is required to estimate possibility of the use of official as a database for creation of the key, I.e. $S=G$.

In also time the use of the grounds G system of double polyadyc number as base information for construction of the key in technology of combined DPP requires the presence of avalanche relating effect consisting of errors appearance at once in the sequence of refurbishable display elements as a result of the incorrectly recovered foundation of one element of DPN.

If $g'_{ij} \neq g_{ij}$, that $|\varepsilon_{\eta\xi} \neq 0$, where $\eta, \xi \in \Omega$ and

$$|\Omega| = \theta \geq 2. \qquad (1)$$

Here Ω is great number of elements positions of DPN, which a condition is executed for $a'_{\eta\xi} \neq \grave{a}_{\eta\xi}$. In other words an error in the process of renewal of one foundation must result in the origin of errors in a few elements of image fragment. Clearly, those errors at renewal of grounds arise up because of unauthorized division.

We will consider the property of the polyadyc system, determined on the basis of expression (1), and questioner the presence of avalanche relating effect, when the incorrectly recovered foundation of one element of double polyadyc number (DPN) must result in the origin of errors in a few elements of image fragment.

For the ground of such property presence we will formulate and will prove a next theorem.

The theorem about an avalanche — relating effect

Incorrectly neat foundation of one of elements of double polyadyc number has influence on the process of renewal elements of DPN, exactly:

1) there is an error in the reconstructed senior elements of DPN, preceding to the element with incorrectly neat foundation, so, that functional dependence between in size errors ε_{ij} and parameters of the polyadyc system is set by the following system:

$$\varepsilon_{ij} = \begin{cases} = -a_{ij} - \dfrac{1}{g'_{\eta\tau}}\Big((g_{ij} g_{\eta\tau} N^{(1,1)}_{(i-1,\,j)} + a_{ij}\, g_{\eta\tau}) \bmod g'_{\eta\tau} - \\ -(g_{ij}\, g_{\eta\tau} N^{(1,1)}_{(i-1,\,j)} + a_{ij}\, g_{\eta\tau}) \bmod (g'_{\eta\tau} g_{ij})\Big), \qquad \rightarrow\ g'_{\eta\tau} > g_{\eta\tau}; \\ -a_{ij} - \dfrac{1}{g'_{\eta\tau}}(g_{ij}\, g_{\eta\tau} N^{(1,1)}_{(i-1,\,j)} + a_{ij}\ g_{\eta\tau} + \dfrac{g_{\eta\tau}\, N^{(i+1,\,j)}_{(\eta-1,\,\tau)} + a_{\eta\tau}}{V^{(i+1,\,j)}_{(\eta-1,\,\tau)}}) \bmod g'_{\eta\tau} + \\ + \dfrac{1}{g'_{\eta\tau}}(g_{ij}\, g_{\eta\tau} N^{(1,1)}_{(i-1,\,j)} + a_{ij}\ g_{\eta\tau} + \dfrac{g_{\eta\tau}\, N^{(i+1,\,j)}_{(\eta-1,\,\tau)} + a_{\eta\tau}}{V^{(i+1,\,j)}_{(\eta-1,\,\tau)}}) \bmod (g_{ij} g'_{\eta\tau}), \rightarrow\ g'_{\eta\tau} < g_{\eta\tau}, \end{cases}$$

where a_{ij} is initial value of $(i; j)$ element of DPN; g_{ij}, $g_{\eta\gamma}$,are grounds for the $(i; j)$ and $(\eta;\tau)$ elements of DPN; $g'_{\eta\gamma}$ it is incorrectly neat foundation for $(\eta;\tau)$ elements of DPN; $N^{(1,1)}_{(i-1,\,j)}$ it is the inlaid value of code-number for the elements of DPN since an element on position $(1;1)$ and concluding by an element on position $((i-1; j)$; $V^{(i+1,j)}_{(\eta-1,\tau)}$; it is the accumulated work of grounds for the elements of DPN since position $(i+1; j)$ and concluding by position with coordinates $(\eta-1;\tau)$.

2) the scopes values which the size of error can adopt concerned on the basis of the following inequality: $-a_{ij} \le \varepsilon_{ij} \le g_{ij} - a_{ij}$;

3) incorrectly neat foundation of DPN element influences on possibility of appearance errors in the process of senior elements renewal of double polyadyc number/I.e., if $g'_{\eta\tau} \neq g_{\eta\tau}$ $\theta \le m(\tau-1)+$, $+\tau\eta$ where θ is amount of the wrong recovered elements of DPN in investigation of wrong neat foundation of $(\eta; \tau)$ element; $m(\tau-1)+\tau\eta$ it is amount of DPN senior elements, preceding to the $(\eta; \tau)$ element.

Proof. On the basis of properties of the polyadyc system flows out, that the gravimetric coefficients of DPN elements do not depend on the grounds of senior elements. Means influencing of incorrect foundation spreads only on senior elements. Therefore we will consider the process of renewal of $(i; j)$ of DPN element on condition that he is senior in relation to an element $(\eta; \tau)$, I.e. inequalities are executed, if $j < \tau$ that $1 \le i \le m$; if $j = \tau$ that $i \le \eta - 1$. We will paint the value of code-number N, selecting in him elements containing elements a_{ij} and $a_{\eta\tau}$:

$$N = \sum_{\xi=1}^{m}\sum_{\gamma=1}^{j-1} a_{\xi\gamma} V_{\xi\gamma} + \sum_{\xi=1}^{i-1} a_{\xi j} V_{\xi j} + a_{ij} V_{ij} + \\ + \sum_{\xi=i+1}^{m} a_{\xi j} V_{\xi j} + \left(\sum_{\xi=1}^{m}\sum_{\gamma=j+1}^{\tau-1} a_{\xi\gamma} V_{\xi\gamma} + \sum_{\xi=1}^{\eta-1} a_{\xi\tau} V_{\xi\tau}\right) + \\ + a_{\eta\tau} V_{\eta\tau} + \left(\sum_{\xi=\eta+1}^{m} a_{\xi\tau} V_{\xi\tau} + \sum_{\xi=1}^{m}\sum_{\gamma=\tau+1}^{n} a_{\xi\gamma} V_{\xi\gamma}\right) \qquad (2)$$

Whereupon we will transform the size of gravimetric coefficient V'_{ij} for the $(i; j)$ element of DPN in obedience to a next formula, $g'_{\eta\tau}$ selecting in her a factor proper to foundation of incorrectly neat element

$$V'_{ij} = \left(\prod_{\xi=i+1}^{m} g_{\xi j} \prod_{\gamma=j+1}^{\tau-1}\prod_{\xi=1}^{m} g_{\xi\gamma}\right) \times \\ \times g'_{\eta\tau} \prod_{\xi=\eta+1}^{m} g_{\xi\tau} \prod_{\gamma=\tau+1}^{n}\prod_{\xi=1}^{m} g_{\xi\gamma}. \qquad (3)$$

Replaceable in correlation for decoding of DPN element size N and V'_{ij} accordingly on expressions (2) and (3), and we will get

$$a'_{ij} = \left[\left(\sum_{\xi=1}^{m} \sum_{\gamma=1}^{j-1} a_{\xi\gamma} V_{\xi\gamma} + \sum_{\xi=1}^{i-1} a_{\xi j} V_{\xi j} + a_{ij} V_{ij} + \sum_{\xi=i+1}^{m} a_{\xi j} V_{\xi j} + \left(\sum_{\xi=1}^{m} \sum_{\gamma=j+1}^{\tau-1} a_{\xi\gamma} V_{\xi\gamma} + \sum_{\xi=1}^{\eta-1} a_{\xi\tau} V_{\xi\tau} \right) + a_{\eta\tau} V_{\eta\tau} + \right.$$

$$\left. + \sum_{\xi=\eta+1}^{m} a_{\xi\tau} V_{\xi\tau} + \sum_{\xi=1}^{m} \sum_{\gamma=\tau+1}^{n} a_{\xi\tau} V_{\xi\tau} \right) \Big/ \left(\prod_{\xi=i+1}^{m} g_{\xi j} \prod_{\gamma=j+1}^{\tau-1} \prod_{\xi=1}^{m} g_{\xi\tau} \right) g'_{\eta\tau} \prod_{\xi=\eta+1}^{m} g_{\xi\tau} \prod_{\gamma=\tau+1}^{n} \prod_{\xi=1}^{m} g_{\xi\gamma} \Bigg] -$$

$$- \left[\left(\sum_{\xi=1}^{m} \sum_{\gamma=1}^{j-1} a_{\xi\gamma} V_{\xi\gamma} + \sum_{\xi=1}^{i-1} a_{\xi j} V_{\xi j} + a_{ij} V_{ij} + \sum_{\xi=i+1}^{m} a_{\xi j} V_{\xi j} + \left(\sum_{\xi=1}^{m} \sum_{\gamma=j+1}^{\tau-1} a_{\xi\gamma} V_{\xi\gamma} + \sum_{\xi=1}^{\eta-1} a_{\xi\tau} V_{\xi\tau} \right) + a_{\eta\tau} V_{\eta\tau} + \right. \right.$$

$$\left. \left. + \sum_{\xi=\eta+1}^{m} a_{\xi\tau} V_{\xi\tau} + \sum_{\xi=1}^{m} \sum_{\gamma=\tau+1}^{n} a_{\xi\gamma} V_{\xi\gamma} \right) \Big/ g_{ij} \left(\prod_{\xi=i+1}^{m} g_{\xi j} \prod_{\gamma=j+1}^{\tau-1} \prod_{\xi=1}^{m} g_{\xi\gamma} \right) g'_{\eta\tau} \prod_{\xi=\eta+1}^{m} g_{\xi\tau} \prod_{\gamma=\tau+1}^{n} \prod_{\xi=1}^{m} g_{\xi\gamma} \right] g'_{\eta\tau} \ . \quad (4)$$

Taking into account

$$\left(\sum_{\xi=\eta+1}^{m} a_{\xi\tau} V_{\xi\tau} + \sum_{\xi=1}^{m} \sum_{\gamma=\tau+1}^{n} a_{\xi\gamma} V_{\xi\gamma} \right)$$

that element, is contribution to the value of code-number from the side of DPN junior elements, and their gravimetric coefficients do not contain foundation $g'_{\eta\tau}$, on the basis of properties of the polyadyc system inequality will be executed

$$\left(\sum_{\xi=\eta+1}^{m} a_{\xi\tau} V_{\xi\tau} + \sum_{\xi=1}^{m} \sum_{\gamma=\tau+1}^{n} a_{\xi\gamma} V_{\xi\gamma} \right) / V'_{ij} < 1.$$

From here painting the relations of the other elements in relation to a size, V'_{ij} and replacing by them in a formula (4) the proper sizes, we will get, if $g'_{\eta\tau} > g_{\eta\tau}$, that

$$V'_{ij} > \sum_{\xi=i+1}^{m} a_{\xi j} V_{\xi j} + \left(\sum_{\xi=1}^{m} \sum_{\gamma=j+1}^{\tau-1} a_{\xi\gamma} V_{\xi\gamma} + \sum_{\xi=1}^{\eta-1} a_{\xi\tau} V_{\xi\tau} \right) +$$

$$+ a_{\eta\tau} V_{\eta\tau} + \sum_{\xi=\eta+1}^{m} a_{\xi\tau} V_{\xi\tau} + \sum_{\xi=1}^{m} \sum_{\gamma=\tau+1}^{n} a_{\xi\gamma} V_{\xi\gamma}.$$

$$a'_{ij} = \left[\frac{g_{ij}\, g_{\eta\tau} N^{(1,1)}_{(i-1,\,j)}}{g'_{\eta\tau}} + \frac{a_{ij}\, g_{\eta\tau}}{g'_{\eta\tau}} \right] -$$

$$- \left[\frac{g_{ij}\, g_{\eta\tau\tau} N^{(1,1)}_{(i-1,\,j)}}{g_{ij}\, g'_{\eta\tau}} + \frac{a_{ij}\, g_{\eta\tau}}{g_{ij}\, g'_{\eta\tau}} \right] g_{ij}.$$

Conclusions

The methodology of semantic structure hiding of images in the decoded — proof systems on the base of double polyadyc presentation as a result of decoding on the by mistake neat grounds of DPN elements, being based on, is developed:

1) forming of the official information system on the base of dynamic ranges of DPN elements , that provides: a) creations of condition for meaningful influence of official information on the process of code-gram forming of informative part;

b) that official information characterize maintenance of the concrete processed local fragment of image.

2) models of avalanche — relating effect in the process of images reconstruction in the combined cryptosemantic systems on the base of polyadyc presentation. Grounded, that incorrectly neat foundation of one of double polyadyc number elements has influence on the process of renewal of DPN elements, namely: there is an error in the reconstructed senior elements of DPN, preceding to the element with incorrectly neat foundation, so, that there is dependence between in size errors and parameters of the polyadyc system, namely from the values of refurbishable element foundation and incorrectly neat foundation, sizes $N^{(i+1,\,j)}_{(\eta-1,\,\tau)}$ and $V^{(i+1,\,j)}_{(\eta-1,\,\tau)}$; the scopes values which the size of error can adopt concerned on the basis of the following inequality: $-a_{ij} \le \varepsilon_{ij} \le g_{ij} - a_{ij}$; incorrectly neat foundation of DPN element influences on possibility of appearance errors in the process of senior elements renewal of double polyadyc number, I.e. if $g'_{\eta\tau} \ne g_{\eta\tau}$, that $\theta \le m(\tau-1)+\tau\eta$; the value of error is the accumulated size, depending on the amount of the distorted grounds participating in the process of the proper element of DPN reconstruction.

References

1. *Gonzalez R.* Digital Image Processing / R. Gonzalez, R. Woods. — M. : Technosphere, 2005. — 1073 p.

2. *Barannik V.* The structurally — combinatory presentation of information in the automated control systems / V. V. Barannik, Y. V. Ctasev, N. A. Koroleva. Monograph, Kharkov: Khups, 2009. — 252 p.

3. *Barannik V.* The methodology of cryptographic transformations creation on the base of the eliminating surplus methods / V. V. Barannik, S. A. Sydchenko, V. V. Larin// The modern special technique, 2009. — №4. — P. 5 — 17.

4. *Barannik V.* Forming of decoded — proof presentation of images in the compression systems / V. V. Barannik, S. A. Sydchenko, V. V. Larin // International Winnitca. — 2010. — P. 40—41.

Стаття надійшла до редакції 11.10.10.