чення і підвищити ефективність побудови відповідних систем виявлення вторгнень.
Ключові слова: кібератаки, аномалії, нечіткі еталони, α-рівневі нечіткі числа, системи виявлення вторгнень, системи виявлення аномалій, системи виявлення атак, виявлення аномалій в комп'ютерних мережах.

THE METHOD OF α-LEVEL OF NOMINALIZATION FOR INTRUSION DETECTION SYSTEMS

Modern facalities which are used for cyber attacks detection in low defined partially formalized environment have a number of limitations. As part of this goal, the appropriate technical solutions are developed for intrusion detection systems, where the basis is the method for anomalies detection caused by cyber attacks in information system. In this method the process of transformation of standards and current fuzzy numbers requires the precise formalization. To overcome this limitation, a method which is based on mathematical models and methods of fuzzy logic and is implemented through three basic stages: formation of α-levels which is equivalent to the conversion of fuzzy numbers, the formation of generelized tables and graphical interpretation of nominalized fuzzy numbers. The method enables to formalize the process of α-level intervals formation to get the equivalent transformation of standard and current fuzzy numbers, which in turn will make it possible to define the identifying terms that indicate the current state of the environment and increase the efficiency of corresponding intrusion detection systems.
Keywords: cyber attacks, anomalies, fuzzy standards, α-level fuzzy numbers, intrusion detection systems, anomaly detection systems, attack detection systems, anomaly detection in computer networks.

Корченко Анна Олександрівна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: annakor@ukr.net
Корченко Анна Александровна, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
Anna Korchenko PhD in Eng., Associate Professor of IT-Security Academic Department, National Aviation University (Kyiv, Ukraine).

УДК 003.26:004.056.5

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ СТІЙКОСТІ МЕТОДУ ПОБІТОВОГО ПРИХОВУВАННЯ ДАНИХ ВІДНОСНО АТАК НА ОСНОВІ АФІННИХ ПЕРЕТВОРЕНЬ

Владислав Ковтун, Олексій Кінзерявий

В даній роботі проведено експериментальне дослідження щодо перевірки стійкості методу побітового приховування даних в структуру векторного зображення відносно атак на основі афінних перетворень. Для проведення експерименту було обрано довільне SVG зображення в структурному складі якого містилися команди побудови кривих Без'є. В одну з цих кривих шляхом її поступового поділу на візуально однакову сукупність сегментів приховувалися дані різного розміру. Над отриманим стеганоконтейнером поступово виконувалися різноманітні афінні перетворення типу перестановка, поворот, зсув за віссю абсцис і ординат, пропорційне та непропорційне масштабування. Одержані результати з перетворення стеганоконтейнера показали, що розглядуваний метод по приховуванню даних у векторні зображення забезпечує стійкість до атак на основі афінних перетворень.
Ключові слова: *захист інформації, цифрова стеганографія, метод побітового приховування даних, векторні зображення, криві Без'є, афінні перетворення.*

Вступ. Розвиток глобальної мережі Інтернет та поширення її використання серед населення планети, сприяє збільшенню обсягів інформації, що передається, обробляється, зберігається та знищується. Інформація може подаватися у різних формах, одна з найпоширеніших – графічні зображення. Растрові зображення, завдяки своїм структурним особливостям, знайшли широке використання в стеганографічних методах захисту інформації в якості контейнера та дозволяють приховувати в собі значні обсяги даних. Однак, до растрових зображень можуть застосовуватися певні графічні перетворення (зміна яскравості, стиснення з втратами, накладання кольорового фільтру, тощо), що можуть впливати на їх структурні та статистичні властивості. Така модифікація може навмисно бути використана як активна атака стеганоаналізу, що спрямована на пошкодження чи знищення секретного повідомлення в стеганоконтейнері. Іншим видом графічних зображень є векторні зображення, які у сучасній стеганографії не поширені.

В роботі [1] запропоновано метод побітового приховування даних в структуру векторного зображення. За яким приховування здійснюється шляхом поступового ділення кривих Без'є на візуально однакові сукупності сегментів, та подальшою заміною сукупністю сегментів початкових кривих векторного зображення. Завдяки властивостям кривих Без'є, такий метод забезпечує теоретичну стійкість до атак на основі афінних перетворень [2]. Однак, при використанні афінних перетворень, на практиці, завжди присутня похибка округлення нових координат векторного зображення. Тому, експериментальне дослідження стійкості методу [1] відносно афінних перетворень є актуальною задачею.

Мета роботи полягає в проведенні експериментального дослідження з перевірки стійкості методу побітового приховування даних в структуру векторного зображення відносно атак на основі афінних перетворень типу перестановка, поворот, зсув за віссю абсцис і ординат, пропорційне та непропорційне масштабування.

Основна частина. Векторні зображення, як і інші види подання графічних зображень (растрове та фрактальне), часто підлягають різним графічним перетворенням. Одними з ключових перетворень векторних об'єктів є накладання певного роду трансформацій, серед яких найбільш поширеними є афінні перетворення. Під афінним перетворенням розуміється перехід від однієї системи координат на площині до іншої, при якому n-вимірний об'єкт відображається в n-вимірний, точка – в точку, лінія – в лінію, поверхня – в поверхню. Так, афінне перетворення для N-вимірного простору в однорідних координатах можна подати за допомогою матричного перетворення:

$$\begin{bmatrix} X_1^* \\ X_2^* \\ \dots \\ X_N^* \\ 1 \end{bmatrix} = \begin{bmatrix} X_1 \\ X_2 \\ \dots \\ X_N \\ 1 \end{bmatrix} \cdot \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \dots & \alpha_{1,N} & \beta_1 \\ \alpha_{2,1} & \alpha_{2,2} & \dots & \alpha_{2,N} & \beta_2 \\ \dots & \dots & \dots & \dots & \dots \\ \alpha_{N,1} & \alpha_{N,2} & \dots & \alpha_{N,N} & \beta_N \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

де X_i – початкові координати заданої точки, $\alpha_{i,j}$ – довільні дійсні числа, що визначають операції повороту, зсуву, масштабування, $\alpha_{i,j} \in R$, β_i – довільні дійсні числа, що визначають операції перестановки, $\beta_i \in R$, $i \in \overline{1,N}$, $j \in \overline{1,N}$.

У подальшому буде розглядатися часний випадок афінних перетворень для *2D* простору ($N = 2$) у системі координат XYZ, де координата $Z = 1$, як матричне перетворення [2, 3]:

$$\begin{bmatrix} X^* \\ Y^* \\ 1 \end{bmatrix} = \begin{bmatrix} X \\ Y \\ 1 \end{bmatrix} \cdot \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \beta_1 \\ \alpha_{2,1} & \alpha_{2,2} & \beta_2 \\ 0 & 0 & 1 \end{bmatrix}.$$

На рис. 1 зображені типи афінних перетворень для *2D* простору [2, 4, 5].

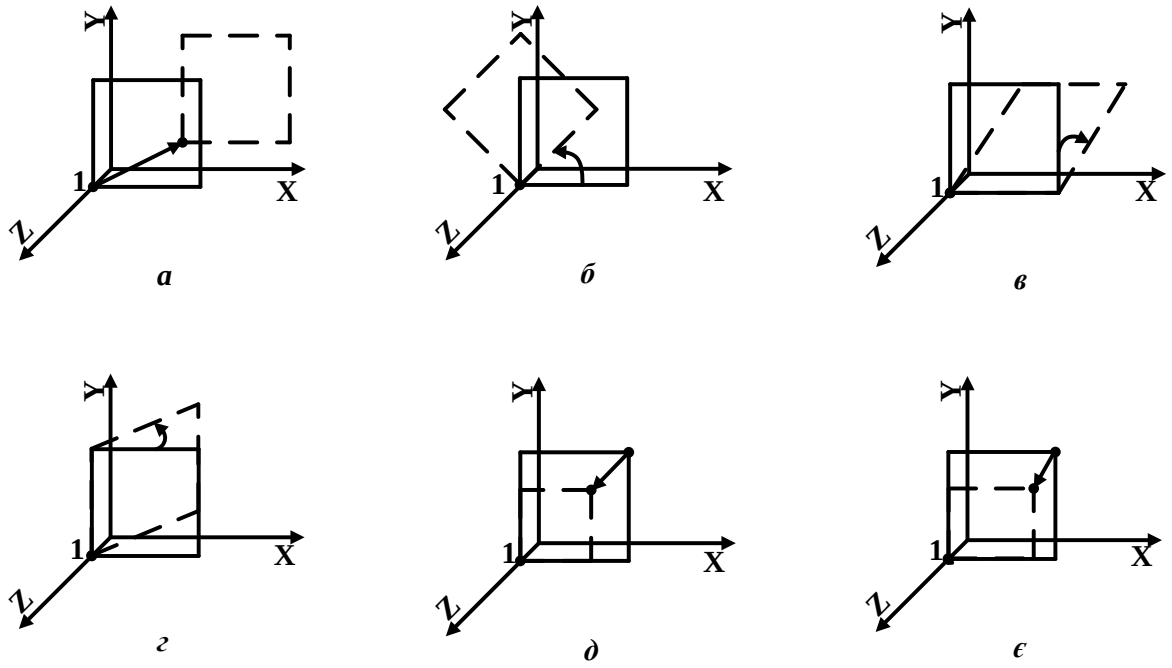

Рис. 1. Типи афінних перетворень для *2D* простору: *а* – перестановка; *б* – поворот; *в* – зсув за віссю абсцис; *г* – зсув за віссю ординат; *д* – пропорційне масштабування; *є* – непропорційне масштабування

За методом [1] здійснюється приховування даних у криві Без'є векторного зображення. Нагадаємо, що будь-яка крива Без'є задається рівнянням [3, 6]:

$$B(t)=\sum_{i=0}^{n} b_{i,n}(t)P_i,\ t=t+\Delta t,\ t\in[0,1],$$

де P_i – опорні точки, $i\in\overline{0,n}$; i – індекс опорних точок; n – порядок визначальної функції базису Бернштейна і сегментів поліноміальної кривої; $n+1$ – кількість опорних точок; t – параметр побудови кривої; Δt – крок зміни параметру t; $b_{i,n}(t)$ – поліноми Бернштейна. Приховування даних відбувається шляхом поступового розбиття початкової кривої на сегменти за алгоритмом де Кастельжо [7] при різних значеннях $t=t+\Delta t$ наступним чином:

– якщо при певному t приховуватиметься біт даних зі значенням "0", то в даній точці поділ кривої Без'є на сегменти не відбуватиметься, а відбудеться перехід до наступного біта приховуваної послідовності та наступного значення t.

– Якщо при певному t приховуватиметься біт даних зі значенням "1", то в даній точці проводиться поділ заданої кривої Без'є на два сегменти. Подальше внесення наступного біту даних приховуваної послідовності відбувається у другий отриманий сегмент кривої при наступному значенні t. Перший сегмент залишається без змін.

– Після приховування даних, отримана послідовність сегментів замінює початкову криву.

Стійкість розглядуваного методу [1] до атак через афінні перетворення забезпечується властивістю, що над будь-якою кривою Без'є можна здійснити будь-яке афінне перетворення, при якому положення та відстані між опорними точками зберігатимуться, але змінюватимуться лише їх координати.

Авторами проведені експериментальні дослідження зі стійкості методу [1] до атак через афінні перетворення. Для дослідження було обрано довільне *SVG* зображення в структурі якого містилися команди побудови кривих Без'є типу curveto [8]. В одну з даних кривих були приховані дані різного розміру (800 та 2000 біт) за використанням ключових параметрів визначених в роботі [8]: максимально допустима кількість розрядів дробової частини числа координат опорних точок кривих Без'є – 12; допустима мінімальна довжини кривої Без'є відносно відстаней між її опорними точками – 5; максимально допустима похибка в кількості останніх розрядів дробової частини числа координат опорних точок – 5.

Після внесення приховуваних даних, до обробленого *SVG* зображення за допомогою графічного редактора "Inkscape" накладалися афінні перетворення типу перестановка, поворот, зсув за віссю абсцис і ординат, пропорційне та непропорційне масштабування.

Афінне перетворення – перестановка

Перестановка векторного об'єкта здійснюється шляхом зміни всіх координат заданого об'єкту на довільне стале значення β_1 за віссю абсцис та на β_2 за віссю ординат за наступною формулою:

$$\begin{bmatrix} X^* \\ Y^* \\ 1 \end{bmatrix} = \begin{bmatrix} X \\ Y \\ 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & \beta_1 \\ 0 & 1 & \beta_2 \\ 0 & 0 & 1 \end{bmatrix}.$$

При проведенні експерименту до обробленого *SVG* зображення поступово накладалися перетворення перестановки з довільними значеннями $\beta_1\in[-500,500]$ та $\beta_2\in[-500,500]$ (тобто до вже зміщеного зображення знову накладалося перетворення перестановки). Було проведено 100 випробувань з накладання даного перетворення на стеганоконтейнер. Після виконання будь-якого з цих перетворень проводилося вилучення даних з перетвореного стеганоконтейнера. Результати експерименту показали, що значення β_1 та β_2 завжди змінюють координати заданого об'єкта на довільні сталі числа та не утворюють похибку округлення при обрахунку нових координат опорних точок, то при вилученні даних завжди отримується повний зміст приховуваного повідомлення. А це означає, що розглядуваний метод [1] забезпечує стійкість до даного перетворення, що і було підтверджено в ході проведення експерименту.

Афінне перетворення – поворот

Поворот векторного об'єкта здійснюється шляхом зміни всіх координат заданого об'єкту на кут θ навколо центра векторного зображення з координатами $(0,0,1)$ за наступною формулою:

$$\begin{bmatrix} X^* \\ Y^* \\ 1 \end{bmatrix} = \begin{bmatrix} X \\ Y \\ 1 \end{bmatrix} \cdot \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

В ході проведення експерименту до обробленого *SVG* зображення поступово накладалися перетворення повороту на кут $\theta=1$ (тобто до вже повернутого зображення знову накладалося перетворення повороту). В загальному було виконано 360 випробувань, в ході яких векторне зображення з приховуваними даними виконувало повне коло обертання навколо свого центру. Після кожного

перетворення повороту проводилася операція з вилучення приховуваних даних з обробленого стеганокотейнера. Одержані результати експерименту показали наступне, що при застосуванні перетворення повороту утворюється похибка округлення значень нових координат опорних точок векторного об'єкта за встановленими вище параметрами. Дана похибка впливає на правильність вилучення даних з зміненого стеганоконтейнера. Результати по визначенню кількості втрачених бітів приховуваного повідомлення при використанні перетворення повороту до стеганоконтейнера приведені на рис. 2.

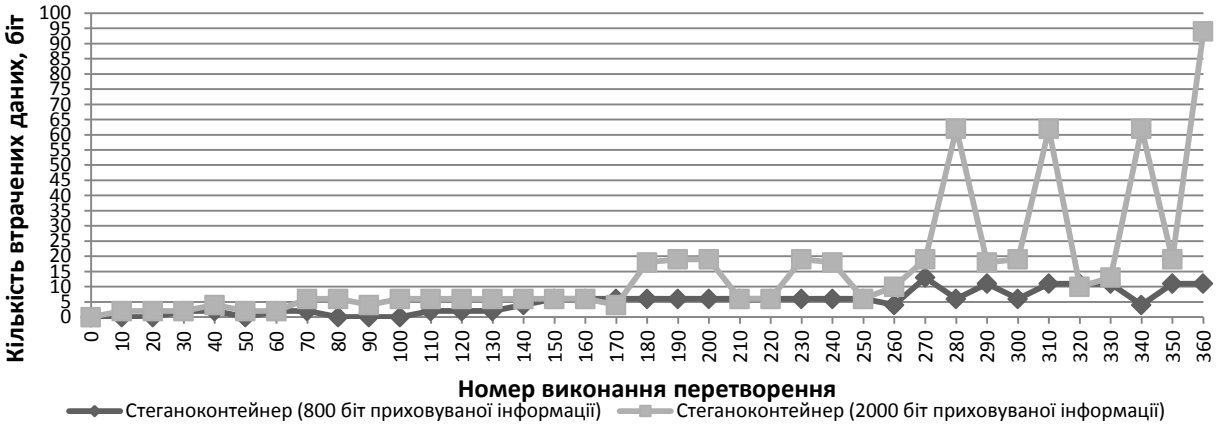

Рис. 2. Результати вилучення даних з стеганоконтейнера після виконання перетворення повороту

Афінне перетворення – зсув

Зсув векторного об'єкта здійснюється шляхом зміщення координат заданого об'єкта за віссю абсцис на певне відсоткове значення $\alpha_{1,2}$ (за віссю ординат на певне відсоткове значення $\alpha_{2,1}$), а координати за віссю ординат (відповідно за віссю абсцис) залишаються без змін. Перетворення зсуву обраховується за однією з наступних формул:

а) зсув за віссю абсцис:

$$\begin{bmatrix} X^* \\ Y^* \\ 1 \end{bmatrix} = \begin{bmatrix} X \\ Y \\ 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & \alpha_{1,2} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

б) зсув за віссю ординат:

$$\begin{bmatrix} X^* \\ Y^* \\ 1 \end{bmatrix} = \begin{bmatrix} X \\ Y \\ 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ \alpha_{2,1} & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

При проведенні експерименту до обробленого *SVG* зображення поступово накладалися перетворення зсуву за віссю абсцис на $\alpha_{1,2} = 0,01$ та за віссю ординат на $\alpha_{2,1} = 0,01$ (тобто до вже зміненого зображення знову накладалися перетворення зсуву). Було проведено 100 випробувань по накладанню кожного перетворення зсуву на стеганоконтейнер, під час яких проводилося вилучення приховуваних даних. У результаті експерименту було встановлено, що перетворення зсуву також утворює похибку округлення при обрахунку нових координат опорних точок векторного об'єкта, а одержані результати по визначенню кількості втрачених бітів приховуваного повідомлення приведені на рис. 3 та рис. 4.

Рис. 3. Результати вилучення даних зі стеганоконтейнера після виконання перетворення зсуву за віссю абсцис

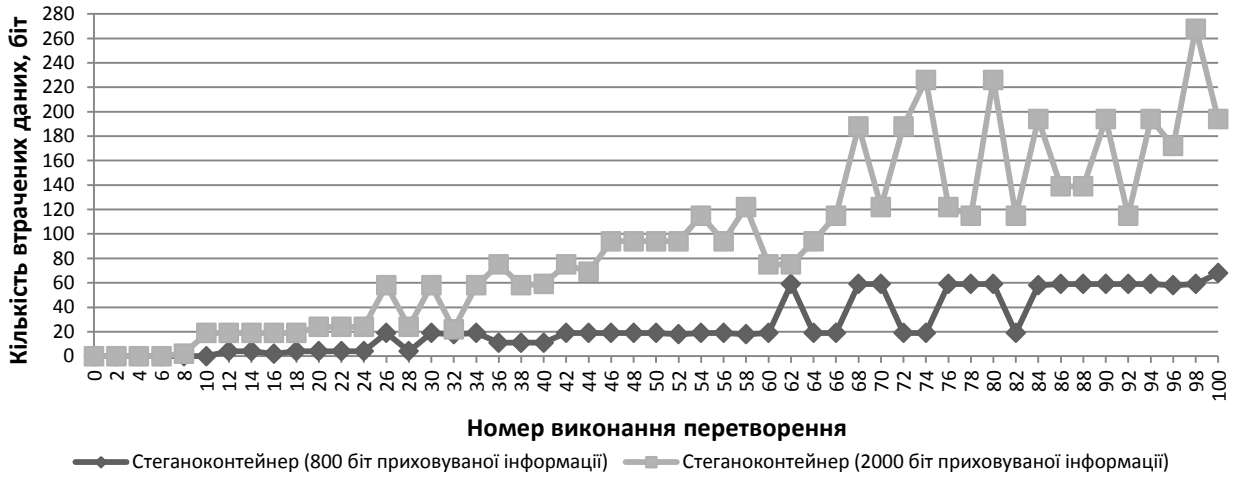

Рис. 4. Результати вилучення даних з стеганоконтейнера після виконання перетворення зсуву за віссю ординат

Афінне перетворення – масштабування

Масштабування векторного об'єкту здійснюється шляхом розтягування / стискання заданого об'єкта вздовж координатних осей при довільних значеннях $\alpha_{1,2}$ та $\alpha_{2,1}$ за наступною формулою:

$$\begin{bmatrix} X^* \\ Y^* \\ 1 \end{bmatrix} = \begin{bmatrix} X \\ Y \\ 1 \end{bmatrix} \cdot \begin{bmatrix} \alpha_{1,1} & 0 & 0 \\ 0 & \alpha_{2,2} & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Якщо $\alpha_{1,1} = \alpha_{2,2}$, то відбувається пропорційне масштабування об'єкту, що при $\alpha_{1,1} = \alpha_{2,2} > 1$ рівномірно розтягується (збільшується), а при $\alpha_{1,1} = \alpha_{2,2} < 1$ рівномірно стискається (зменшується). Якщо $\alpha_{1,1} \neq \alpha_{2,2}$, то відбуватиметься непропорційне масштабування.

При проведенні експерименту до оброблених *SVG* зображень поступово накладалися перетворення пропорційного та непропорційного масштабування. Було проведено 200 випробувань по кожному з видів масштабування (тобто до вже зміненого зображення знову накладалося перетворення зміни масштабу того же типу). При яких векторне зображення з приховуваними даними поступово стискалося / розширювалося з такими значеннями:

– $\alpha_{1,1} = 0{,}99$, $\alpha_{2,2} = 0{,}99$ при пропорційному стиску векторного зображення та $\alpha_{1,1} = 1{,}01$, $\alpha_{2,2} = 1{,}01$ при пропорційному розтягуванні векторного зображення;

– $\alpha_{1,1} = 0{,}99$, $\alpha_{2,2} = 1$ при непропорційному стиску векторного зображення по осі абсцис та $\alpha_{1,1} = 1{,}01$, $\alpha_{2,2} = 1$ при непропорційному розтягуванні векторного зображення по осі абсцис;

– $\alpha_{1,1} = 1$, $\alpha_{2,2} = 0{,}99$ при непропорційному стиску векторного зображення по осі ординат та $\alpha_{1,1} = 1$, $\alpha_{2,2} = 1{,}01$ при непропорційному розтягуванні векторного зображення по осі ординат.

Результати експерименту по визначенню кількості втрачених бітів приховуваного повідомлення приводяться на рис. 5, рис. 6 та рис. 7.

Рис. 5. Результати по вилученню даних з стеганоконтейнера після виконання перетворення пропорційного масштабування

Рис. 6. Результати по вилученню даних з стеганоконтейнера після виконання перетворення непропорційного масштабування по осі абсцис

Рис. 7. Результати по вилученню даних з стеганоконтейнера після виконання перетворення непропорційного масштабування по осі ординат

Окремим випадком масштабування є перетворення дзеркального відображення. Яке полягає в відбиванні векторного об'єкта на інших квадрантах координатної площини при різних значеннях $\alpha_{1,1} \in \{-1,1\}$, $\alpha_{2,2} \in \{-1,1\}$. При проведені експерименту з 100 випробувань по застосуванню даного перетворення було встановлено, що при накладанні даного перетворення змінюються лише знаки координат опорних точок векторного об'єкта, а самі значення лишаються не змінним. Одержані результати експерименту показали, що при накладанні дзеркального перетворення на стеганоконтейнер завжди при вилученні даних отримується повний зміст секретного повідомлення. А це означає, що розглядуваний метод [1] є стійким до даного роду перетворень.

Висновки. Одержані результати свідчать, що розглянутий метод [1] завдяки властивостям кривих Без'є забезпечує стійкість до атак на основі афінних перетворень типу перестановка, поворот, за віссю абсцис і ординат, пропорційне та непропорційне масштабування.

З отриманих результатів експерименту було встановлено наступне:

1. Розглядуваний метод [1] є стійким до афінних перетворень типу перестановка та дзеркальне відображення. Оскільки, дані перетворення не утворюють похибок округлення при обрахунку нових координат опорних точок векторного об'єкта.

2. Перетворення повороту, зсуву за віссю абсцис і ординат, пропорційного та непропорційного масштабування утворюється похибка округлення при обчисленні нових координат опорних точок векторного об'єкта при встановлених ключових параметрів. Тому, при багаторазовому їх використанні виникає не значна втрата частини приховуваних даних при вилученні їх з обробленого стеганоконтейнера. З зменшенням розміру приховуваних даних в одну криву Без'є векторного зображення тим збільшується його стійкість і

зменшуються втрати приховуваних даних при накладанні даних перетворень.

ЛІТЕРАТУРА

[1]. Кінзерявий О.М. Стеганографічний метод приховування даних у векторних зображеннях / О.М. Кінзерявий, В.Ю. Ковтун, С.О. Гнатюк, В.М. Кінзерявий // теоретичний і науково-практичний журнал "Вісник Інженерної академії України". – 2013. – №3-4. – С. 66-68.

[2]. Маценко В.Г. Комп'ютерна графіка: [навч. посібник] / В.Г. Маценко. – Ч.: Рута, – 2009. – 343 с.

[3]. Голованов Н.Н. Геометрическое моделирование / Н.Н. Голованов. – М. : издательство Физико-математической литературы, – 2002. – 472 с.

[4]. Бахрушина Г.И. Моделирование геометрических атак на основе аффинных преобразований / Г.И. Бахрушина // электронное научное издание "Ученые заметки ТОГУ". – 2013. – Т.4, №4. – С. 1291-1297.

[5]. Яглом И.М. Идеи и методы аффинной и проективной геометрии : [часть I] // И.М. Яглом, В. Г. Ашкинузе. – М. : Учпедгиз, – 1962. – 248 с.

[6]. Роджерс Д. Математические основы машинной графики : [пер. с англ.] / Д. Роджерс, Дж. Адамс. – М. : Мир, – 2001. – 604 с.

[7]. Кунву Ли Основы САПР (CAO/CAM/CAE) / Ли Кунву. – СПб. : Питер, – 2004. – 560 с.

[8]. Кінзерявий О.М. Експериментальне дослідження методу побітового приховування даних у векторні зображення / О.М. Кінзерявий, В.Ю. Ковтун // науковий журнал "Безпека інформації". – 2014. – Т.20, №1. – С. 66-70.

REFERENCES

[1]. Kinzeryavyy O.M., Kovtun V.Y., Gnatyuk S.O., Kinzeryavyy V.M. (2013) "Steganography method of hiding data in vector images", Bulletin of Engineering Academy of Ukraine, №3-4, pp. 66-68.

[2]. Matsenko V.G. (2002) "Computer Graphics", *Ch.: Ryta*, 343 p.

[3]. Golovanov N.N. (2002) "Geometric modeling", *M.: publishing house of physicomathematical literature*, 472 p.

[4]. Bakhrushina G.I. (2013) "Modeling geometric attacks based on affine transformations", Scientists notes PNU, VOL. 4 №4, pp. 1291-1297.

[5]. Yaglom I.M., Ashkinuze V.G. (1962) "The ideas and methods of the affine and projective geometry", *M.: Uchpedgiz,* 248 p.

[6]. Rodjers D., Adams J. (2001) "Mathematical Foundations of Computer Graphics", *M.: Mir,* 604 p.

[7]. Kunvu Lee (2004) "Basics CAD (CAO / CAM / CAE)", *St.P. : Peter*, 560 p.

[8]. Kinzeryavyy O.M., Kovtun V.Y. (2014) "Experimental research of bitwise method for information hiding in vector images", Information Security, VOL. 20 №1, pp. 66-70.

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ СТОЙКОСТИ МЕТОДА ПОБИТОВОГО СОКРЫТИЯ ДАННЫХ ОТНОСИТЕЛЬНО АТАК НА ОСНОВЕ АФФИННЫХ ПРЕОБРАЗОВАНИЙ

В данной работе проведено экспериментальное исследование по проверке устойчивости метода побитового сокрытия данных в структуру векторного изображения относительно атак на основе аффинных преобразований. Для проведения эксперимента было выбрано произвольное SVG изображение, в структурном составе которого находились команды построения кривых Безье. В одну из этих кривых, путем ее постепенного разделения на визуально одинаковую совокупность сегментов, скрывались данные разного размера. Над полученным стеганоконтейнером постепенно выполнялись различные аффинные преобразования типа перестановка, поворот, смещение по оси абсцисс и ординат, пропорциональное и непропорциональное масштабирование. Полученные результаты по преобразованию стеганоконтейнера показали, что рассматриваемый метод по сокрытию данных в векторные изображения обеспечивает устойчивость к атакам на основе аффинных преобразований.

Ключевые слова: защита информации, цифровая стеганография, метод побитового сокрытия данных, векторные изображения, кривые Безье, аффинные преобразования.

AN EXPERIMENTAL STUDY OF THE STABILITY OF THE BITWISE DATA HIDING METHOD, RELATIVE TO ATTACKS, BASED ON AFFINE TRANSFORMATIONS

In this work an experimental study was conducted to verify the stability of the bitwise data hiding method in the structure of vector image, relative to attacks, based on affine transformations. The arbitrarily SVG image, in the structural composition of which were the commands of constructing Bezier curves, was chosen for the experiment. In one of these curves, by its gradual separation into a visually identical aggregate of segments, were hiding data of different sizes. The various affine transformations such as permutation, rotation, offset along the abscissa and ordinate, proportional and non-proportional scaling were gradually performed over received steganocontainer. The received results for the transformation of the steganocontainer showed that the considered method of hiding data in vector images provides resistance to attacks based on affine transformations.

Index terms: information security, digital steganography, bitwise method of data hiding, vector images, Bezier curves, affine transformations.

Ковтун Владислав Юрійович, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: vladislav.kovtun@gmail.com.

Ковтун Владислав Юрьевич, кандидат технических наук, доцент кафедры безопасности информационных технологий Национального авиационного университета.
Vladislav Kovtun, Ph.D., Assossiate Professor of IT-Security Academic Department, National Aviation University.

Кінзерявий Олексій Миколайович, аспірант кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: oleksiykinzeryavyy@gmail.com.
Кинзерявый Алексей Николаевич, аспирант кафедры безопасности информационных технологий Национального авиационного университета.
Kinzeryavyy Oleksiy, postgraduate student of IT-Security Academic Department, National Aviation University.

УДК 004.056:159.95

МОДЕЛЬ ТА МЕТОДИ ЗАХИСТУ СТРУКТУРОВАНОЇ СОЦІАЛЬНОЇ ГРУПИ ВІД НЕГАТИВНОГО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

Анатолій Шиян, Юрій Яремчук

Структуровані соціальні групи (ССГ) виділені в якості специфічного об'єкту дослідження внаслідок того, що саме вони є найбільш вразливою мішенню для здійснення негативного інформаційно-психологічного впливу. При цьому сама ССГ функціонує як потужний підсилювач для того інформаційно-психологічного впливу, який було здійснено на її вище керівництво. Побудовано модель для здійснення діяльності ССГ із врахуванням наявності її ієрархічної будови. Враховано, що в таких ССГ люди діляться на дві категорії: координатори (які можуть створювати нову для ССГ інформацію або адекватно відновлювати її) та тиражувальники (які можуть лише, в найкращому випадку, передати інформацію далі без викривлень). Це призводить до того, що кількість людей на кожному вищому ієрархічному рівні складає порядку 6% від їх кількості на нижчому рівні. Розроблено методи захисту ССГ від негативного інформаційно-психологічного впливу, які враховують їх специфічні риси. Серед них такі: економічна діяльність організацій, діяльність суспільних інститутів, врахування також і гетерархічної будови ССГ, врахування часових рамок функціонування людини як координатора в ССГ, обмеження механізмів демократії тощо.
***Ключові слова**: інформаційно-психологічна безпека, структурована соціальна група, ієрархія, діяльність, управління.*

Вступ. Структуровані соціальні групи є поширеною ціллю для здійснення негативного інформаційно-психологічного впливу. Найбільшу небезпеку становить здійснення негативного інформаційно-психологічного впливу людей, що знаходяться на вищих рівнях в ієрархічно структурованій соціальній групі: тоді вся соціальна група виступає в якості надзвичайно потужного «підсилювача» відповідного негативного впливу. В результаті такі впливи, хоч і орієнтовані на дуже обмежено коло людей, здатні становити серйозну загрозу інформаційній безпеці суспільства та держави в цілому.

Для ефективній протидії інформаційним загрозам такого виду необхідно розробити ефективну модель, яка здатна описати інформаційні процеси в ієрархічній соціальній групі та прийняття рішень в ній. Основна проблема полягає в необхідності здійснити моделювання для специфічних особливостей опрацювання інформації особами, які знаходяться на вищих ієрархічних рівнях. Емпіричний досвід людства свідчить, що далеко не кожна людина здатна здійснювати ефективну діяльність на вищих рівнях управління в соціальній групі, але теоретичне осмислення відстає від практики дуже сильно.

Таким чином, побудова моделей опрацювання інформації в ієрархічно структурованій соціальній групі та розробка методів її захисту від негативного інформаційно-психологічного впливу є актуальною науковою та важливою в практичному плані задачею.

Аналіз останніх досліджень і публікацій. Цю проблему висвітлено в багатьох публікаціях вітчизняних та зарубіжних авторів, серед яких слід виділити Д. Асемоглу, В.М. Богуша, В.Л. Бурячка, С. Гельбаха, А.А. Кобозєву, П. Конотопова, М. Кузнєцова, Ю. Курносова, Л. Нікіфорову, С. Расторгуєва, Дж. Робінсона, В.О. Хорошка, О.К. Юдіна та інших фахівців.

Так, існують фундаментальні книги із інформаційної безпеки держави [1, 2], в яких викладено основні технології для аналізу та прийняття рішень в предметній області інформаційної без-