

5. Schaller J. Single machine scheduling with family setups to minimize total earliness and tardiness / Jeffrey E. Schaller, Jatinder N.D. Gupta // *European Journal of Operational Research*. – 2008. – Vol. 187, № 3. – Pp. 1050-1068.

6. Baker K.R. Sequencing with earliness and tardiness penalties: a review / K.R. Baker, G.D. Scudder // *Operations Research*. – 1990. – № 38(1). – Pp. 22-36.

7. Ващук Ф.Г. Складання розкладів груп для одного приладу із налагодженнями за критерієм мінімізації сумарного випередження і запізнення / Ф.Г. Ващук, О.А. Павлов, О.Б. Місюра, О.О. Мельник // *Вісник Національного технічного університету України "ХПІ"*. – Темат. вип.: "Системний аналіз, управління та інформаційні технології". – Харків: Вид-во НТУ "ХПІ". – 2011. – № 32. – С. 8-18.

8. Ващук Ф.Г. Складання розкладів сумарного випередження і запізнення із налагодженнями, що залежать від послідовності / Ф.Г. Ващук, О.А. Павлов, О.Б. Місюра, О.О. Мельник // *Вісник Національного технічного університету України "ХПІ"*: зб. наук. праць. – Сер.: Інформатика, управління та обчислювальна техніка. – К.: Вид-во "Век+". – 2011. – № 53. – С. 192-194.

9. Ващук Ф.Г. Дослідження ефективності алгоритму складання розкладів сумарного випередження і запізнення із налагодженнями, що залежать від послідовності / Ф.Г. Ващук, О.О. Мельник // *Бионика интеллекта. Информация, язык, интеллект*. – Харьков: Изд-во ХНУРЭ. – 2012. – № 1(78). – С. 49-52.

10. Мельник О.О. Дослідження властивостей алгоритмів складання розкладів груп для одного приладу із налагодженнями за критерієм сумарного випередження і запізнення / О.О. Мельник // *Вісник Східноукраїнського національного університету імені Володимира Даля*: зб. наук. праць. – 2012. – № 2 (173). – С. 241- 246.

11. Мельник О.О. Дослідження властивостей алгоритму складання розкладів за критерієм сумарного випередження і запізнення із налагодженнями, що залежать від послідовності / О.О. Мельник // *Технічні науки та технології: наук. журнал / Черніг. нац. технол. ун-тет*. – 2015. – № 1 (1). – С. 126-130.

Мельник Е.А. Эвристические алгоритмы решения одноэтапных задач составления расписаний для усовершенствования модели многоуровневой системы планирования

Проанализированы эвристические алгоритмы решения задач теории расписаний по критерию минимизации суммарного опережения и запаздывания с учетом наладки приборов. Решена актуальная научно-практическая задача усовершенствования модели многоуровневой системы планирования с сетевым представлением технологических процессов и ограниченными ресурсами за счет включения в третий уровень модели заданий с наладками приборов. Исследована эффективность представленных алгоритмов в сравнении с известным точным методом. Приведен пример практического применения разработанных алгоритмов.

Ключевые слова: информационные технологии, теория расписаний, одноэтапные задачи, системы планирования, наладка оборудования, критерий минимизации суммарного опережения и запаздывания.

Melnyk O.O. Heuristic Algorithms for Resolving of One-stage Scheduling Tasks in Improvement of Multilevel Planning System

This article is devoted to heuristic algorithms for resolving of one-stage scheduling tasks according to the criterion of minimizing the total earliness and tardiness, taking into account the equipment adjustment. We resolve the actual scientific and practical objective regarding the improvement of multilevel planning system with network representation of technological processes and limited resources by means of inclusion to the third level the model of tasks with adjustment. The effectiveness of represented algorithms was researched comparing to the well-known exact method. The example of practical application of created algorithms is represented.

Keywords: information technologies, scheduling theory, one-stage problem, planning systems, device adjustment, criteria of minimizing of the total earliness-tardiness.

УДК 004.056.5:655.25

Доц. М.А. Назаркевич, д-р техн. наук;
аспір. О.А. Троян – НУ "Львівська політехніка"

МЕТОД ЗАХИСТУ ДОКУМЕНТІВ НА ОСНОВІ ЕФЕКТУ МУАРУ

В інформаційній безпеці держави важливу роль відіграє захист друківаних документів. Розроблено спеціальні графічні побудови, на основі яких створено елементи з ефектом муару, що підвищують ефективність і надійність захисту. Розглянуто можливість поліпшити результати захисту за допомогою використання ефекту муару для підвищення ефективності захищеності документів. Цей метод зможе забезпечити високий рівень захисту інформації в друкованому або електронному вигляді, не залишаючи можливості фальсифікації навіть на сучасних копіювальних пристроях. Технологія захисту передбачає створення захисних елементів на основі виникнення муарних решіток у разі спроби фальсифікації документу. Технологію розроблено на етапі підготовки друкованих та електронних документів до друку.

Ключові слова: захист інформації, захисний елемент, друк, муар.

Вступ. Захист інформації на сьогодні набуває вагомого значення на державному рівні¹. Інформація в електронному чи друкованому вигляді потребує новітніх захищених способів від фальсифікації. На теперішньому етапі розвитку інформаційних технологій стає дедалі легше сфальсифікувати будь-яку документацію. Отже, щоб підвищити рівень захисту, потрібно розробляти нові методи, відтворення яких потребує багато часу та зусиль. Щоб захист був ефективним, він має задовольняти критерії надійності та економічності. Чим вищий ступінь захисту, тим тяжче її підробити. Сучасні технології дають змогу підробити буквально все, але тоді виникає питання чи вартує підробка затрачених зусиль та коштів. Основна мета захисту – зробити підробку нерентабельною. Зрозуміло, що зростання якості захищеності документів веде до підвищення вартості фальсифікації. Отже, розглянувши різні випадки захисту документів, можна прийти до висновку, що розробляти захищений документ потрібно з урахуванням максимального захисту та рентабельності.

Мета роботи – розробити технологію захисту для документів на паперових та електронних носіях.

Об'єкти досліджень – друковані та електронні документи (бланки, посвідчення, документи, що потребують захисту).

Аналіз останніх досліджень і публікацій. Відомо, що захищений документ має володіти властивостями:

- *конфіденційності* – бути захищеним від несанкціонованого ознайомлення;
- *цілісності* – бути захищеним від несанкціонованого спотворення, руйнування або знищення;
- *доступності* – бути захищеним від несанкціонованого блокування [1].

На електронний чи друкований документ можуть здійснюватися такі загрози: фальсифікація документа; втрата деякої інформації; заміна деякої інформації; копіювання паперового носія; оцифрування даних; заміна документу. Тому можна ідентифікувати такі загрози: часткова підробка; повна підробка; фальсифікація документу; фальсифікація персоналізованих атрибутів і реквізитів документа; крадіжка.

¹ Публікація містить результати досліджень, проведених за грантової підтримки Державного фонду фундаментальних досліджень за конкурсним проектом.

Загальноприйняті методи управління загрозами: стратегічне управління; тактичне управління. Документ, залежно від ступеня захищеності, може перебувати у: контрольованому оточенні; неконтрольованому оточенні; професійному оточенні. Внаслідок цього пропонуємо рекомендації щодо управління, тобто формуємо методіку протидії визначеній множині загроз та формуємо політику безпеки документа. На рис. 1 показано формування комплексу засобів захисту у системі захисту інформації для друкованих та електронних документів, які перебувають у зовнішньому середовищі. Щоб захистити інформацію, розробляємо програмне забезпечення, яке здійснювало б захист електронних та документів на етапі додрукарської підготовки.

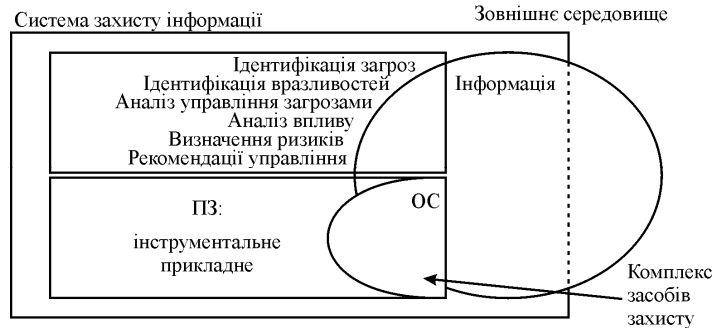


Рис. 1. Аналіз формування загроз

Результати дослідження. Спосіб захисту полягає у створенні тонких паралельних ліній зі шириною 0,25 мм та частотами повторень, які кратні цілому числу частоти відтворювального пристрою і відрізняються від частоти копіювання/сканування на величину менше 0,25 мм, що візуально неможливо розпізнати без використання спеціальних оптичних пристроїв [2]. За такого створення документ володітиме графічними захисними ознаками. Паперовий носій, який містить захисні елементи, має хоча б одне захисне зображення, котре складається з великої кількості видимих і окремо надрукованих елементів, утворених з кривих ліній та фрагментів, які формують захисний об'єкт. Технологія захисту передбачає, що документ буде надрукований поліграфічним способом зі захисними елементами. Коли зловмисник намагатиметься сфальсифікувати документ, на захисних елементах утвориться муар – поява решітки (рис. 2).

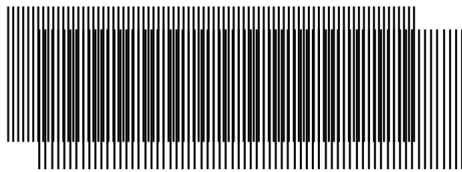


Рис. 2. Поява муару

Можемо змінювати ширину ліній залежно від щільності сірого кольору оригінального зображення. Якщо ж у рівновіддалених лініях змінювати кут нахилу, то можна спостерігати муар у вигляді решіток, які змінюватимуть нахил.

На рис. 3 представлені муарні ефекти, утворені з кутами нахилу 5°, 15°, 45°. Як видно з малюнків, муарна решітка набуває різного вигляду та форми.

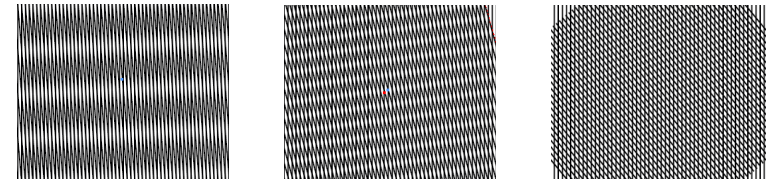


Рис. 3. Муарні ефекти, утворені з кутами нахилу 5°, 15°, 45°

Наявність муарових елементів спотворює вигляд документа, що призводить до значних змін форми чи повної втрати елементів зображення на копії, що дає змогу візуально легко відрізнити фальшиву копію від оригіналу. Якщо частота ліній перевищує 0,7-0,8 мм, що відповідає пороговій частоті візуального сприйняття, то такий фрагмент зображення візуально сприймаються півтоновим. Основна ідея методу захисту полягає в тому, що для захисних елементів формують зміщення частини ліній муару на половину величини кроку лінії [3]. Муар повинен відображатись, коли кут буде малим, тим чіткіше він буде відтворюватися під час фальсифікації документів.

За комбінації кількох шарів рівновіддалених ліній отримують муар, сформований під різними кутами нахилу ліній. Муар проявляється у вигляді решіток, вигляд яких представлено на рис. 4.

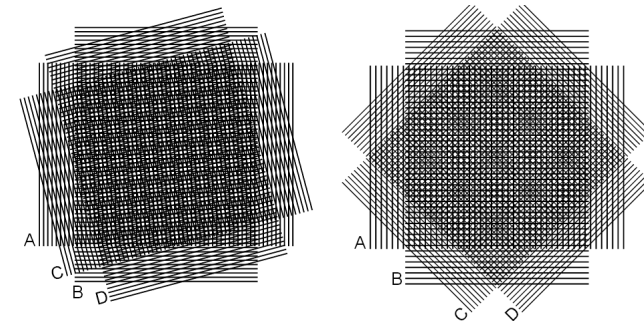


Рис. 4. Муар, який створений комбінацією накладання шарів рівновіддалених ліній під різними кутами

Отримання таких муарних ефектів важко прогнозувати, оскільки ефект сильно залежить від технічних характеристик та налаштувань обладнання, що використовується для відтворення. Дослідимо ефект муару детальніше. Муарові лінії створюються від перетину базового та допоміжного шару [4], що показано на рис. 5.

Базовий шар містить лінії, які рівновіддалені з періодом T_r і знаходяться під кутом α_r до початку відліку системи координат. Допоміжний шар матиме період повторення ліній T_b і з нахилом α_b . У разі накладання базового та допоміжного шарів створюється муарна решітка, яку показано пунктирною лінією. На рис. 5 показано, що вузли муарної решітки матимуть довжину l та знаходитимуться під кутом α_m . Проекції на вісь ординат базового та допоміжного шарів p_b та p_r .

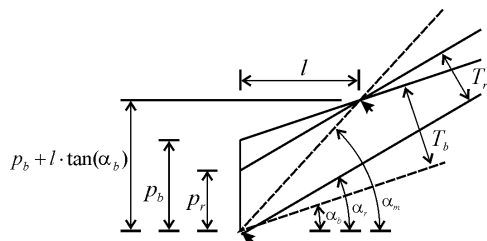


Рис. 5. Схема утворення муарових ліній, які залежать від кута нахилу α базового та допоміжного шарів

Відомо, що

$$\begin{cases} \tan \alpha_m = \frac{p_b + l \cdot \tan \alpha_b}{l} \\ \tan \alpha_r = \frac{p_b - p_r + l \cdot \tan \alpha_b}{l} \end{cases} \quad (1)$$

Отже

$$\tan \alpha_m = \frac{p_b \cdot \tan \alpha_r - p_r \cdot \tan \alpha_b}{p_b - p_r} \quad (2)$$

З тригонометричних відношень маємо

$$T_b = p_b \cdot \cos \alpha_b; T_r = p_r \cdot \cos \alpha_r; T_m = p_m \cdot \cos \alpha_m.$$

Підставивши у (2) отримуємо

$$\alpha_m = \arctan \left(\frac{T_b \cdot \sin \alpha_r - T_r \cdot \sin \alpha_b}{T_b \cos \alpha_r - T_r \cos \alpha_b} \right) \quad (3)$$

Після певних перетворень отримуємо

$$T_m = \frac{T_b \cdot T_r}{\sqrt{T_b^2 + T_r^2 - 2 \cdot T_b \cdot T_r \cdot \cos(\alpha_r - \alpha_b)}} \quad (4)$$

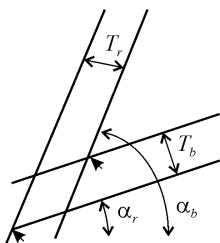


Рис. 6. Дві решітки є ідентичними, $T_b = T_r$

Базовий та допоміжний шари побудовані однаково, отже, їхні періоди збігаються, тобто $T_b = T_r$. Якщо дві решітки є ідентичними (рис. 6), то обґрунтуємо формування муару, коли базовий та допоміжний шари решіток зміщуються під певним кутом, а їх періоди збігаються [5].

Першу сітку повертатимемо на кут α_r , а другу – на α_b .

З (4) отримуємо

$$T_m = \frac{T_b^2}{\sqrt{2T_b^2 - 2 \cdot T_b^2 \cdot \cos(\alpha_r - \alpha_b)}} \quad (5)$$

Після перетворень отримуємо

$$T_m = \frac{T_b}{\sqrt{2 \cdot (1 - \cos(\alpha_r - \alpha_b))}} = \frac{T_b}{\sqrt{2 \cdot (\cos \alpha_r \cos \alpha_b + \sin \alpha_r \sin \alpha_b)}}; \quad (6)$$

Якщо прийняти, що $\alpha_r = 0$, то $\cos \alpha_r = 1$

$$T_m = \frac{T_b}{\sqrt{2 \cdot \cos \alpha_b}} \quad (8)$$

З (3) при $\alpha_r = 0$, $T_b = T_r$ випливає:

$$\alpha_m = \arctan \left(\frac{\sin \alpha_r}{\cos \alpha_r - 1} \right) \quad (9)$$

Побудуємо з (9) залежність зміни кута муарної решітки α_m від кута нахилу базової решітки α_r . При $\alpha_r = 0$ решітки збігаються, муар не відтворюється. На рис. 7 введено α_r , яке змінюється в межах від $-\pi/2$ до $\pi/2$. Побудуємо залежність зміни періоду муарної решітки у випадку коли періоди базового та основного шарів сіток ідентичні. Цю залежність описано (8).

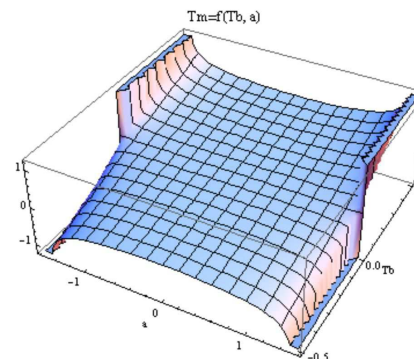


Рис. 7. Залежність періоду зміни муарної решітки T_m від кута нахилу решітки базового шару α_b та періоду базового шару T_b

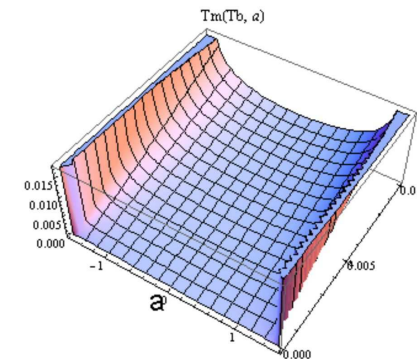


Рис. 8. Залежність періоду зміни муарної решітки T_m від кута нахилу решітки базового шару α_b та періоду базового шару $T_b \in [0..0,01]$

На рис. 8 показано залежність періоду зміни муарної решітки T_m від кута нахилу решітки базового шару α_b та періоду базового шару T_b , з якого випливає, що у випадку малих змін кута нахилу базового та основного шарів муарна решітка [6] різко змінює свій період. З графіка випливає, що чим менший період решітки базового шару, тим величина муарної решітки є помітніша та більша, що проілюстровано на рис. 8. Тому для подальших досліджень було обрано період зміни ліній базового шару $T_b \in [0..0,01]$.

Висновки. Розроблено нову технологію захисту друкованих та електронних документів, яка передбачає створення захисних елементів на основі виникнення муарних решіток у разі спроби фальсифікації документа. Техноло-

гію розроблено на етапі підготовки друкованих та електронних документів до друку. Проведено дослідження виникнення муарних решіток у документі. Захисні елементи створюються на основі муару, який формується двома структурами з паралельних ліній. Розроблено математичні моделі формування муару та обґрунтовано його виникнення. Запропонований метод захисту може бути реалізований стандартними апаратними та програмними засобами. Метод є економічно обґрунтованим і надійним.

Література

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р., № 80/94-ВР. [Чинний, поточна ред. від 30.04.2009 р.] // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.
2. Коншин А.А. Защита полиграфической продукции от фальсификации / А.А. Коншин. – М.: ООО "Синус", 1999. – 157 с.
3. Назаркевич М. Аналіз сучасних методів та програмних ужитків з графічним захистом друкованих документів / Марія Назаркевич, Оксана Троян // Технічні вісті : зб. наук. праць. – 2013. – № 1 (37). – С. 42-44.
4. Назаркевич М. Розроблення методу захисту документів латентними елементами на основі фракталів / М. Назаркевич, І. Дронюк, О. Троян, Т. Томашук // Захист інформації : зб. наук. праць. – 2015. – № 1. – С. 81-85.
5. Назаркевич М.А. Розроблення програмного продукту для захисту інформації на основі плівок із прихованим латентним зображенням / М.А. Назаркевич, О. Троян // Вісник Національного університету "Львівська політехніка". – Сер.: Комп'ютерні науки та інформаційні технології. – Львів : Вид-во НУ "Львівська політехніка", – 2014. – № 806. – С. 187-194.
6. Gabrielyan Emin. The basics of line moiré patterns and optical speedup / Emin Gabrielyan // Scientific Park of Swiss Federal Institute of Technology, 2007. – 9 p.

Назаркевич М.А., Троян О.А. Метод защиты документов на основе эффекта муара

В информационной безопасности государства важную роль играет защита печатных документов. Разработаны специальные графические построения, на основе которых созданы элементы с эффектом муара, повышающие эффективность и надежность защиты. Рассмотрена возможность улучшить результаты защиты посредством использования эффекта муара для повышения эффективности защищенности документов. Данный метод сможет обеспечить высокий уровень защиты информации в печатном или электронном виде, не оставляя возможности фальсификации даже на современных копировальных устройствах. Технология защиты предусматривает создание защитных элементов на основе возникновения муарных решеток при попытке фальсификации документа. Технология разработана на этапе подготовки печатных и электронных документов в печать.

Ключевые слова: защита информации, защитный элемент, печать, муар.

Nazarkevych M.A., Troyan O.A. Document Protection Method based on Moiré Effect

State protection of printed documents plays an important role in information security. There are special graphic constructions based on which a moiré effect of items that increase the efficiency and reliability of protection. The possibility to improve the results of protecting by using moiré effect in order to strengthen documents security is studied. This method can provide a high level of data protection in printed or electronic form, leaving no possibility for falsification even in modern copiers. Protection technology involves creating protective elements based on origin moiré grids while trying forgery. The technology developed in preparation of printed and electronic documents to print.

Keywords: information security, security features, printing, moiré effect.

УДК 614.8

Проф., вед. научн. сотр. Б.Б. Поспелов, д-р техн. наук;

адъюнкт Р.М. Полстянкин – НУ гражданской защиты Украины, г. Харьков

МЕТОД ДВОЙНОГО ДЕТЕКТИРОВАНИЯ ЗАГОРАНИЙ В ПРИРОДНЫХ ЭКОСИСТЕМАХ НА ОСНОВЕ ГРУППЫ ДИСТАНЦИОННЫХ СЕНСОРОВ

Рассмотрен метод двойного детектирования загораний в природных экосистемах на основе использования группы дистанционных сенсоров и его байесовская оптимизация. Проведено решение задачи оптимизации байесовского правила двойного детектирования для групповых сенсоров при фиксированном пороге первичного детектирования. Исследованы зависимости порога и мажоритарного правила детектирования в различных условиях наблюдения физического компонента загорания. Произведена количественная оценка ожидаемого выигрыша при оптимизации двойного детектирования загорания.

Ключевые слова: двойное детектирование, групповой сенсор, физический компонент загорания, мешающие факторы.

Постановка проблемы. Одним из основных направлений сокращения ущерба от природных пожаров в экосистемах является дистанционный мониторинг состояния лесов и торфяников. Для этой цели в мировой практике последних лет предлагается использовать множество беспроводных сенсоров, размещаемых на контролируемой площади, которые способны автономно измерять физические компоненты возможных очагов загорания и дистанционно передавать на контрольный пункт информацию об их состоянии. Применение таких систем сталкивается с проблемой наличия ошибок при обнаружении критических состояний измеряемых физических компонентов загорания в виде пропусков и ложных срабатываний. В связи с этим проблема обеспечения эффективного мониторинга лесов и торфяников для Украины становится особо актуальной. Приоритетным направлением решения данной проблемы следует считать снижение ошибок при раннем обнаружении критических состояний измеряемых физических компонентов загорания. Наиболее конструктивным в этом направлении является подход, базирующийся на объединении автономных сенсоров в реальные или виртуальные группы – создании групповых сенсоров, в которых решение о наличии или отсутствии критического состояния выносится на основе метода двойного детектирования загорания. При этом на первом этапе решается задача первичного детектирования критического состояния каждым из сенсоров группы, а на втором – производится второе детектирование, при котором выносится окончательное решение о наличии или отсутствии загорания на контролируемой площади. В связи с необходимостью повышения эффективности двойного детектирования загораний в экосистемах, с одной стороны, а также сложность условий измерения физических компонентов загорания, снижающая эффективность их детектирования – с другой стороны, порождают проблему оптимизации процедуры двойного детектирования загораний для групповых сенсоров.

Анализ последних исследований и публикаций. В работе [1] для повышения эффективности обнаружения пожара предлагается объединение сенсоров в группу с последующим применением мажоритарного правила обработки информации от сенсоров. При этом возможности снижения ошибочных ре-