ІНФОКУМУНІКАЦІЙНІ ТЕХНОЛОГІЇ, АВТОМАТИЗАЦІЯ ТА ОБЧИСЛЮВАЛЬНА ТЕХНІКА В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ

УДК 004.522
DOI: 10.31891/2219-9365-2019-63-1-39-44

МУЛЯР І. В.,
БОТВІН В. Ю.
Хмельницький національний університет

МЕТОДИ ІДЕНТИФІКАЦІЇ ОСОБИ КОМП'ЮТЕРНИМ ЗОРОМ ТА ЇХ ОПТИМІЗАЦІЯ

На сьогоднішній день що раз частіше застосовуються системи біометричної ідентифікації. Практично всі сучасні смартфони обладнанні сенсором відбитку пальця, а в деяких інших це розпізнавання райдужної оболонки ока. А також все частіше застосовується розпізнавання обличчя користувача. В статті запропоновано метод, за допомогою якого можна використовувати звичайну WEB-камеру з метою ідентифікації людей для доступу до помешкання, використовуючи їх біометричні дані. В будинку з такою системою людині досить буде лише підійти до дверей, система розпізнає обличчя і відімкне двері. А також розглянуто розпізнання людей комп'ютерним зором. Було проаналізовано компанії, що займаються ідентифікацією біометричними даними для отримання доступу.

Зараз на ринку представлена велика кількість пристроїв, що входять до складових розумного дому. Ряд компаній електронних гігантів вкладають значні інвестиції в дану сферу. Було розглянуто пристрої з цієї категорії, і виявилось, що немає аналогічної технології, яка б змогла надати доступ до помешкання за допомогою візуального підтвердження особи. Це підтверджує актуальність розробки і знайде застосування. Суть розробки полягає в тому, що звичайна WEB-камера під'єднана до вічка дверей передає інформацію на блок управління, який в свою чергу відмикає замок в разі відповідності зображення такому в бібліотеці «білого списку». Наразі альтернативи не було представлено для широкого застосування. Також є варіант модифікації даної системи для збільшення енергоефективності додавши модуль детектора руху для активації. А також додати інфрачервоні світлодіоди для можливості використання в темну або мало освітлену пору доби. Інфрачервоне світло невидиме для людського ока і чудово сприймаються цифровими камерами, що не спровокує дискомфорту в особи перед пристроєм. Побудова пристрою пропонується на базі міні-комп'ютера.

Ключові слова: розумний будинок, штучний інтелект, замок, ідентифікація.

MULYAR I. V.,
BOTVIN V. YU.
Khmelnytskyi National University

METHODS OF IDENTIFICATION OF A PERSON WITH COMPUTER VISION AND THEIR OPTIMIZATION

Nowaday biometric identification systems are more commonly used. Almost all modern smartphones are equipped with fingerprint sensor, and in some others it is the recognition of the iris of the eye. Also increasingly used facial recognition user. The article proposes a method by which a regular WEB camera can be used to identify people to access the home using their biometric data. In a house with such a system, a person will only have to approach the door, the system recognizes the face and unlock the door. And also the recognition of people by computer vision is considered. Now the market is represented by a large number of devices that are part of a smart home. A number of e-giant companies invest heavily in this area. Devices from this category were considered, and it turned out that there is no similar technology that could provide access to the home through visual confirmation of a person. This confirms the relevance of the development and will find application. The essence of the development lies in the fact that the usual WEB camera connected to the door of the cell transmits information to the control unit which in turn unlocks the lock if the image matches the image in the whitelist library. At present, alternatives have not been presented for widespread use. There is also an option for modifying this system to increase energy efficiency by adding a motion detector module for activation. And also add infrared LEDs for use in dark or slightly illuminated times of the day. Infrared light is invisible to the human eye and is well received by digital cameras, which does not cause discomfort in the person before the device. The device is powered by a mini-computer.

Keywords: smart home, artificial intelligence, lock, identification.

Постановка проблеми. Ідентифікація особи комп'ютерним зором застовується для аутентифікації користувача в системі. Здавалося б що на даний час є багато алгоритмів для ідентифікації, але постає необхідність оброки потокового відео з подальшим визначенням особи в режимі online для підтвердження користувача для подальшого надання доступу.

Аналіз останніх джерел. Аналізуючи методи, які зараз застосовуються, виявлено кілька алгоритмів для визначення людини і їх практичне застосування.

Першим практичним застосуванням класифікації в відеопотоці став аналіз глядачів для систем Digital Signage – цифрових екранів, встановлених у громадських місцях, в основному для розповсюдження

реклами. Завдяки аналізу кількості глядачів та їх статі/віку з'явилася можливість об'єктивно оцінювати ефективність конкретних екранів і рекламних роликів. Оскільки для вирішення цього завдання достатньо, визначати тільки людей, що дивляться в екран протягом як мінімум пари секунд, то зображення осіб, що подаються на вхід класифікації, виходять відносно фронтальними і чіткими.

Подібні рішення вже досить поширені і пропонуються низкою компаній. У першу чергу варто виділити систему Intel AIM Suite[1] – вона створена на основі розробок канадської компанії CognoVision, купленої Intel в 2010 р. за 25 млн дол. Intel використовує модель Software as a Service (SaaS), пропонуючи послугу аналізу аудиторії за ціною 20 дол. за один екран (одну камеру) на місяць.

Альтернативні рішення пропонуються в тому числі ізраїльською компанією TruMedia Technologies, іспанськими AITech і Inspecta, російської Rhonda Software.

У Росії активно використовують системи, що дозволяють вирішити частину завдання – оцінити кількість відвідувачів. Це досягається за рахунок використання камер на стелі, спрямованих вертикально вниз. Завдяки такому ракурсу виходить надійно підраховувати людей навіть при щільному потоці. Відповідні рішення пропонують вже багато російських компаній – itseez, "Сінезіс", "ЕЛВІС-Неотек", "Сателіт Інновація", Rhonda Software та ін. Однак у всіх цих системах відсутня можливість класифікації людей, оскільки обличчя людини при такому ракурсі не видно зовсім.

Trueface.AI [2] – Виявлення шахрайства. Інколи технологія розпізнавання обличчя може не розрізняти обличчя людини та фотографію. Як результат, цей недолік може суттєво поставити під загрозу зусилля безпеки. Прагнучи вирішити цю проблему, Trueface.AI, розробники розпізнавання обличчя дзвінок називається Chui [3], використовують глибоке навчання та технологію розпізнавання обличчя, щоб відрізнити обличчя людини від фотографії.

Kairos [4, 5] – виявлення шахрайства. Можливо, одна з найбільших компаній у сфері розпізнавання обличчя AI, Kairos використовує машинне навчання та комп'ютерне бачення, щоб запускати свій набір інструментів, що включають в себе стандартні функції розпізнавання обличчя та інші параметри, такі як стать, вік та етнічні ознаки. У 2015 році компанія придбала за 2,7 мільйона доларів США IMRSV (компанія-програма), яка, як повідомляється, "перетворює будь-яку веб-камеру на інтелектуальний сенсор".

MasterCard Identity Check Mobile app[6] - безпека облікового запису. Паролі стали обтяжливими при використанні Інтернет-середовища. MasterCard є однією з фінансових установ, які бажають уникнути необхідності в отриманні паролів через розпізнавання осіб. MasterCard Identity Check Mobile зазвичай перевіряє онлайн-платежі за допомогою відбитків пальців або розпізнавання осіб. Користувачі програми можуть перевіряти свої платежі використовуючи свою камеру для смартфонів, щоб сфотографувати своє обличчя.

Метою роботи є розв'язання задачі комп'ютерної ідентифікації людини на основі аналізу зображення обличчя в режимі реального часу. Для досягнення поставленої мети розглянуто представлені методи ідентифікації та обрано метод гнучкого порівняння на графах.

Виклад основного матеріалу. Метод гнучкого порівняння на графах [7] (Elastic graph matching) зводиться до еластичному зіставлення графів, що описують зображення осіб. Особи представлені у вигляді графів зі зваженими вершинами та ребрами. На етапі розпізнавання один з графів – еталонний – залишається незмінним, в той час як інший деформується з метою найкращої підгонки до першого. У подібних системах розпізнавання графи можуть являти собою як прямокутну сітку, так і структуру, утворену характерними (антропометричними) точками особи.

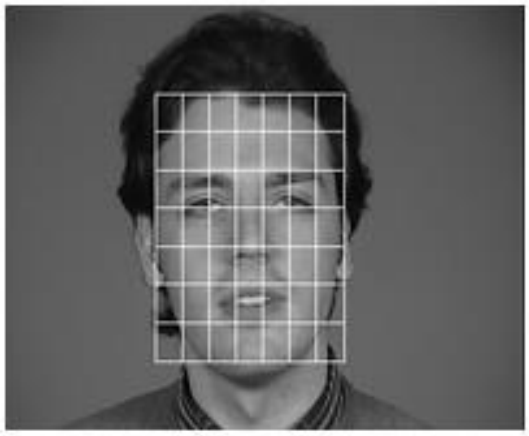


Рис. 1а. Регулярна сітка

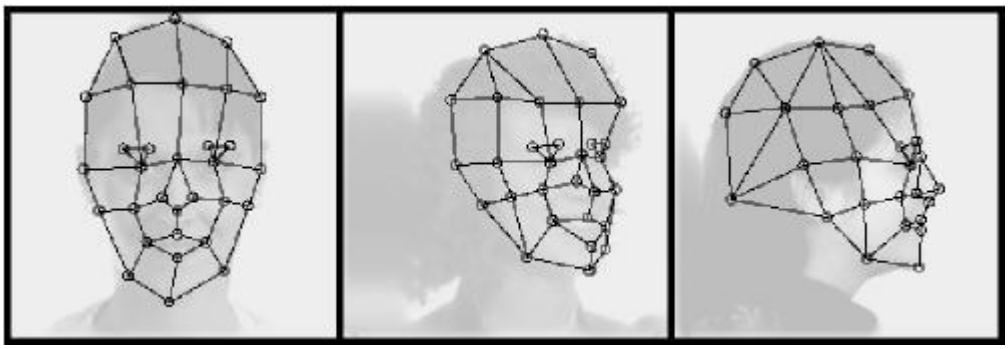


Рис. 1б. Граф на основі антропометричних точок обличчя

У вершинах графа обчислюються значення ознак, найчастіше використовують комплексні значення фільтрів Габора або їх впорядкованих наборів – Габорівских вейвлет (строї Габора), які обчислюються у деякої локальної області вершини графа локально шляхом згортки значень яскравості пікселів з фільтрами Габора.

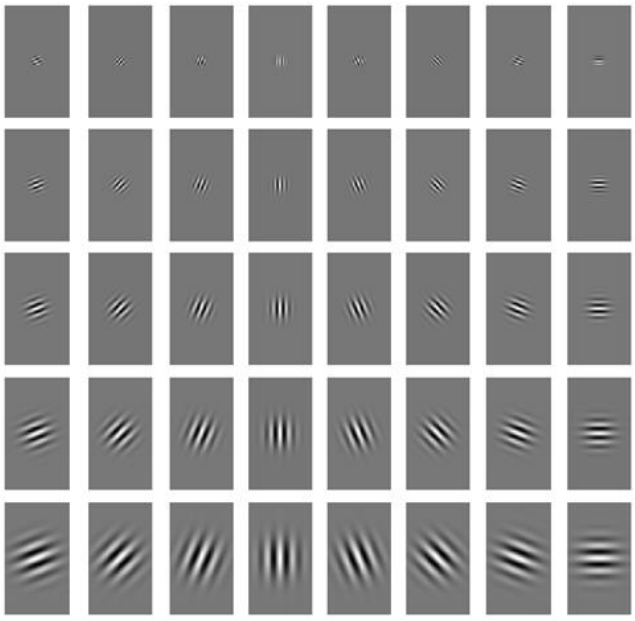


Рис. 2. Набір (банк, jet) фільтрів Габора

Ребра графа зважуються відстанями між суміжними вершинами. Різниця (відстань, дискримінаційна характеристика) між двома графами обчислюється за допомогою деякої функції цінової деформації, що враховує як розходження між значеннями ознак, обчисленими в вершинах, так і ступінь деформації ребер графа.

Деформація графа відбувається шляхом зміщення кожної з його вершин на деяку відстань в певних напрямках щодо її початкового місця розташування і вибору такої позиції, при якій різниця між значеннями ознак (відгуків фільтрів Габора) у вершині деформованого графа і відповідної їй вершині еталонного графа буде мінімальною. Дана операція виконується по черзі для всіх вершин графа до тих пір, поки не буде досягнуто найменша сумарна різниця між ознаками деформованого і еталонного графів. Значення цінової функції деформації при такому положенні графа, що деформується, і буде мірою відмінності між вхідним зображенням обличчя і еталонним графом. Дана «релаксаційна» процедура деформації повинна виконуватися для всіх еталонних осіб, закладених в базу даних системи. Результат розпізнавання системи – еталон з найкращим значенням цінової функції деформації.

В окремих публікаціях вказується 95-97% - а ефективність розпізнавання навіть за наявності різних емоційних виразах і зміні ракурсу обличчя до 15 градусів. Однак розробники систем еластичного порівняння на графах посилаються на високу обчислювальну вартість даного підходу. Наприклад, для порівняння вхідного зображення обличчя з 87 еталонними витрачалося приблизно 25 секунд при роботі на паралельній ЕОМ з 23 трансп'ютерами [8] (примітка: публікація датована 1993 роком). В інших публікаціях з даної тематики час або не вказується, або кажуть, що воно велике.

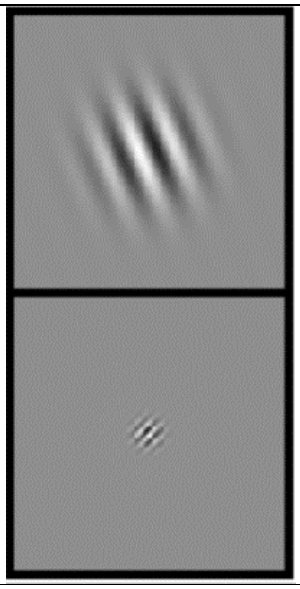
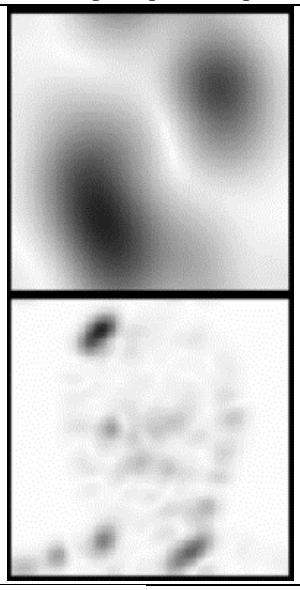
Вхідне зображення	Приклад двох фільтрів Габора	Результат звертання вхідного зображення обличчя і фільтрів Габора
		

Рис. 3. Приклад згортки зображення особи з двома фільтрами Габора

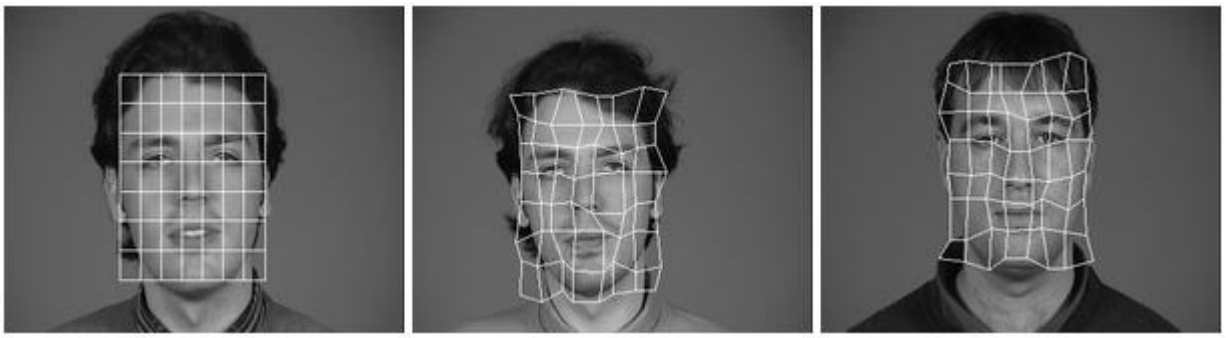


Рис. 4. Приклад деформації графа у вигляді регулярної решітки

Даний метод сегментації заснований на застосуванні серії фільтрів Габора. Відмінною особливістю даного фільтра є те, що він здатний виділяти прямі лінії певного розміру і під певним кутом.

Дійсна частина цього фільтра виглядає наступним чином:

$$g(x, y, \lambda, \psi, \sigma, \gamma) = exp\left(-\frac{x'^2+\gamma^2 y'^2}{2\sigma^2}\right)cos\left(2\pi\frac{x}{\lambda}+\psi\right)$$

де $x' = x\cos\theta + y\sin\theta$;
$y' = x\sin\theta + y\cos\theta$;
x,y – координати центру ядра в наперед заданих межах;
λ – період ядра в пікселях;
θ – нахил ядра;
σ – дисперсія Гауссіана;
ψ – зміщення фази ядра;
γ – стиснення Гауссіана.

Таким чином, щоб виділити образ, потрібно застосувати фільтр Габора з різними кутами нахилу ядра і порахувати максимальний відгук кожного пікселя на серію фільтрів.

За Габором застосовується малоефективний метод запису голограм зображений на рисунку 5а.

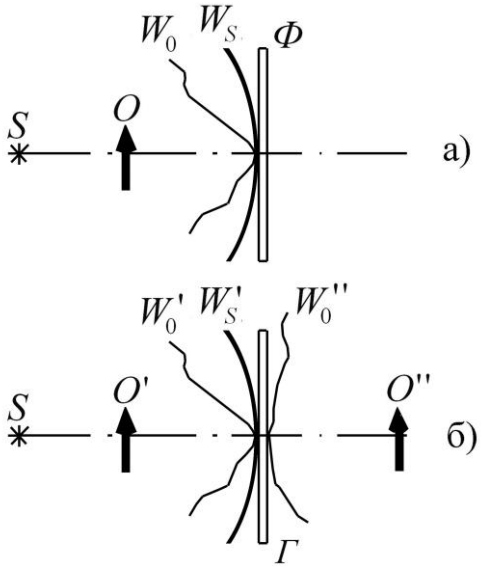


Рис. 5. Схема запису (а) та відновлення (б) за Габором

При освітлені об’єкта *О* монохромним джерелом *S* на фотопластині *Ф* реєструється розсіяна від об'єкта хвиля W_0 і референтна хвиля від джерела світла W_S.

При реконструкції голограми Габора зображеної на рисунку 5б), проявлена і експонована голограма *Г* встановлюється на те ж місце, яке вона займала при зйомці і на неї направляється випромінювання когерентного джерела *S.* Падаючи на голограму, це випромінювання модулюється її малюнком так, що за голограмою відновлюється хвиля $W`_0$, випромінювання, розсіяного об'єктом і, відповідно, з'являється зображення об'єкта *О*, невідмінного від оригіналу. Крім істинного зображення, виникає також і фальшиве *О’’*, яке розташовується між спостерігачем та істинним зображенням. В результаті накладання та взаємного впливу цих зображень обидва вони сильно спотворюються.

Виникнення помилкового зображення є прямим наслідком принципових недоліків методу відтворення фаз за рахунок виключення «непотрібних» частин референтної хвилі.

Оптимізація алгоритму досягається за рахунок обробки зображення фільтром Габора шляхом усереднення значень оброблюваного зображення за деякою області в кожній точці. відповідно, накладення фільтра Габора на зображення має вид:

$$I`(x,y)=\frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}I\left(x-\frac{n}{2}+i,y-\frac{n}{2}+j\right)G(i,j)$$

Підібраний фільтр Габора представлений на рисунку 6 і задається формулою:

$$Filter(x,y)=\exp\left(-\frac{x`^2+100y`^2}{2*49}\right)\cos(2\pi x`+90)$$

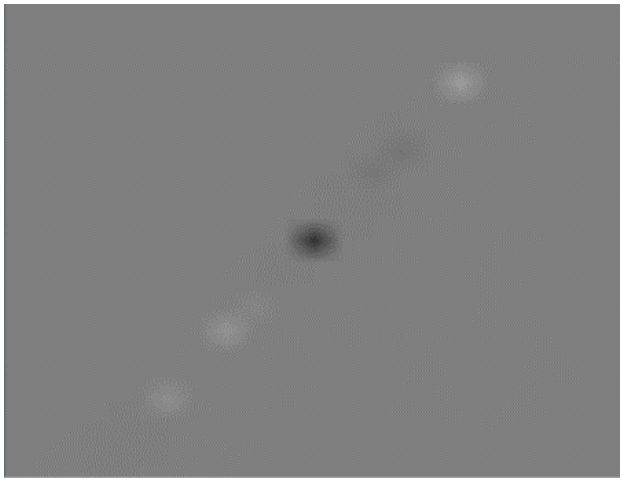


Рис. 6. Графічне представлення фільтру Габора

В результаті застосування даного фільтру вдалось виокремити характерні риси обличчя. Далі до результатів фільтрації необхідно застосувати алгоритми аналізу зображення. Наприклад алгоритм Фрімена [9], для виділення контуру зображення, відфільтрованого Габорівським фільтром, для виділення на вихідному зображенні обличчя.

Висновки. Метод Габора має ряд незаперечних переваг перед більшістю інших: при досить високій точності визначення він дозволяє проводити перевірку на відстані, допускає таємну перевірку і вимагає наявності тільки відеокамери. Розроблено досить велике число алгоритмів, що забезпечують не тільки високу швидкодію і точність визначення, але і дозволяють системі працювати в самих різних умовах. Сукупність цих якостей зумовила дуже швидкий розвиток цього методу, поставивши його за поширеністю в один ряд з дактилоскопічної перевіркою.

Виникає необхідність модифікації методу для проведення ідентифікації і авторизації за умов поганого освітлення та надання доступу для користувача.

Проаналізовано існуючі методи розпізнавання обличь на зображеннях, а також найбільш поширені методи фільтрації зображення. Продемонстровано доцільність застосування фільтрів Габора для фільтрації зображень з метою виділення на них обличь.

Наукова новизна дослідження полягає в розробці ефективного методу виявлення обличь з отриманням інформації про їх біометричні властивості. Сутність запропонованого методу полягає в фільтрації вихідного зображення, застосуванні порогової обробки, виділення контурів отриманого об'єкту на зображенні і підтвердженні особи з білого списку.

Практичне застосування цього методу може бути використане як складову розумного будинку, «розумний замок», який ідентифікує особу і на основі проведеного аналізу оптичного зображення виносе рішення про надання чи ненадання доступу до помешкання.

Література

1. Intel® to Launch AIM Suite Anonymous Video Analytics Technology [Electronic resource]. URL: https://aimsuite.intel.com/resources/knowledge-base
2. TruMedia’s solutions specific knowledge that includes the passers & shoppers [Electronic resource]. URL: www.trumedia.co.il
3. Chui the facial recognition Doorbell [Electronic resource]. URL: http://my-smarthome.com/en/smart-home-products/chui-the-facial-recognition-doorbell
4. Implement Face Recognition into dozens of products [Electronic resource]. URL: https://trueface.ai/about
5. Realtime Video Analysis [Electronic resource]. URL: https://trueface.ai/facerecognition
6. Mastercard Identity Check: Facial Recognition Biometrics [Electronic resource]. URL: https://newsroom.mastercard.com/videos/mastercard-identity-check-facial-recognition-biometrics
7. Face Recognition by Elastic Bunch Graph Matching [Electronic resource]. URL: http://www.face-rec.org/algorithms/ebgm/wisfelkrue99-facerecognition-jainbook.pdf
8. Distortion invariant object recognition in the dynamic link architecture [Electronic resource]. URL: https://ieeexplore.ieee.org/document/210173
9. Сообщество любителей робототехники Robocraft [Electronic resource]. URL: http://robocraft.ru.

References

1. Intel® to Launch AIM Suite Anonymous Video Analytics Technology [Electronic resource] URL: https://aimsuite.intel.com/resources/knowledge-base
2. TruMedia’s solutions specific knowledge that includes the passers & shoppers [Electronic resource] URL: www.trumedia.co.il
3. Chui the facial recognition Doorbell [Electronic resource] URL: http://my-smarthome.com/en/smart-home-products/chui-the-facial-recognition-doorbell
4. Implement Face Recognition into dozens of products [Electronic resource] URL: https://trueface.ai/about
5. Realtime Video Analysis [Electronic resource] URL: https://trueface.ai/facerecognition
6. Mastercard Identity Check: Facial Recognition Biometrics [Electronic resource] URL: https://newsroom.mastercard.com/videos/mastercard-identity-check-facial-recognition-biometrics
7. Face Recognition by Elastic Bunch Graph Matching [Electronic resource] URL: http://www.face-rec.org/algorithms/ebgm/wisfelkrue99-facerecognition-jainbook.pdf
8. Distortion invariant object recognition in the dynamic link architecture [Electronic resource] URL: https://ieeexplore.ieee.org/document/210173
9. Community of robotics lovers Robocraft [Electronic resource] URL: http://robocraft.ru.

Рецензія/Peer review : 27.11.2018 Надрукована/Printed : 04.02.2019
Рецензент: д. т. н, проф. Говорущенко Т. О.