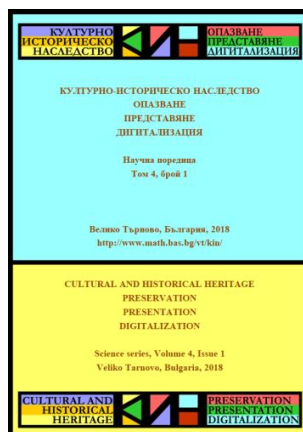


Science series
**Cultural and Historical
Heritage:
Preservation,
Presentation,
Digitalization**
Volume 4, Issue 1, 2018

Editors
Petko St. Petkov
Galina Bogdanova

**Institute of Mathematics and
Informatics, BAS**

RPL "P. R. Slaveykov"
Veliko Tarnovo, Bulgaria



ISSN: 2367-8038
Web: <http://www.math.bas.bg/vt/kin/>

Научна поредица
**Културно-историческо
наследство:**
**опазване,
представяне,
дигитализация**
Том 4, брой 1, 2018

Редактори
Петко Ст. Петков
Галина Богданова

**Институт по математика
и информатика, БАН**

РНБ „П. Р. Славейков“
Велико Търново, България

Galina Bogdanova, Nikolay Noev

**Protection of Digital Resources in the Field of Cultural Heritage
in Libraries, Museums, Archives and Galleries in Northern and Central
Bulgaria**

Pages 168-181

Галина Богданова, Николай Ноев

**Защита на цифрови ресурси в областта на културното нас-
ледство в библиотеки, музеи, архиви и галерии в Северна и Цент-
рална България**

Страници 168-181

http://www.math.bas.bg/vt/kin/files/papers/4_1/12-KIN-4-1-2018.pdf

Материалите в сборника са обект на авторско право.

Разрешение за направа на електронни или хартиени копия на част или на цяла публикация за лично или обучително ползване се предоставя без заплащане, при условие, че копията не са направени или разпространявани с цел печалба или търговска изгода и че копията са съпроводени с това съобщение и пълно цитиране на първата страница. За копиране под друга форма, за препубликуване или публикуване на сървъри се изисква предварително специално разрешение и/или заплащане.

Том 4, брой 1, 2018, ISSN: 2367-8038, <http://www.math.bas.bg/vt/kin/>

Научни редактори:

проф. д-р Петко Ст. Петков, доц. д-р Галина Богданова

Технически редактори:

гл. ас. д-р Николай Ноев, гл. ас. д-р Калина Сотирова-Вълкова, гл. ас. д-р Галия Георгиева-Цанева, Паскал Пиперков

© Авторски колектив, 2018

Издание на:

Институт по математика и информатика към Българска академия на науките
Регионална народна библиотека „П. Р. Славейков”, гр. В. Търново, България
Съюз на учените в България, клон Велико Търново, България

This work is subject to copyright.

Permission to make digital or hard copies of portions of this work for personal or classroom use is granted without fee, provided that the copies are not made or distributed for profit or commercial advantage and that the copies bear this notice and the full citation on the first page. To otherwise reproduce or transmit in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage retrieval system or in any other way requires written permission from the publisher.

Volume 4, Issue 1, 2018, ISSN: 2367-8038, <http://www.math.bas.bg/vt/kin/>

Editors:

Prof. Phd. Petko St. Petkov, Assoc. prof. Phd. Galina Bogdanova

Copy editors:

Assist. prof. Phd. Nikolay Noev, Assist. prof. Phd. Kalina Sotirova-Valkova, Assist. prof. Phd. Galya Georgieva-Tsaneva, Paskal Piperkov

© Editors, authors of papers, 2018

Published by:

Institute of Mathematics and Informatics at Bulgarian Academy of Sciences
Regional Public Library “P. R. Slaveykov”, Veliko Tarnovo, Bulgaria
Union of scientists in Bulgaria, Veliko Tarnovo branch, Bulgaria

СЪДЪРЖАНИЕ / TABLE OF CONTENT

Предговор	5
Preface.....	7
Съдържание / Table of Content	9
Sabin Popovici , O Ipoteză în Ceea ce Privește Identificarea Proprietarului Villae – I Din Cartierul Artizanal al Romulei.....	11
Sabin Popovici , A Hypothetical Relationship with Regard to the Identification of the Villa's Property's Identification from the Romanian Artisan Cartier.....	11
Светлана Венелинова, Валери Григоров , Селищната система през праисторическата епоха по горното и средното течение на река Голяма Камчия. Етапи и методи на проучване	25
Svetlana Venelinova, Valeri Grigorov , The Settlement System from the Prehistoric Period on the Upper and the Middle Stream of the Golyama Kamchiya River. Stages and Methods of Research	25
Гая Георгиева-Цанева, Галина Богданова , Първи стъпки към използването на облачните изчисления при цифровизацията на културното наследство и осигуряване на сигурността в дигиталната конверсия и съхранение на информацията	57
Galya Georgieva-Tsaneva, Galina Bogdanova , First Steps to the Use of Cloud Computing in Digitalization of Cultural and Historical Heritage and Security in the Digital Conversion and Storage of Information	57
Донка Колева , Читалища от 19 век – домове за просвещение и национално съзнание, пазители на българските традиции.....	69
Donka Koleva , 19 th Century Community Centres (Chitalishta) – Homes of Enlightenment and National Consciousness, Guardians of Bulgarian Traditions.....	69
Павлина Владева , 30 години клуб по битова култура „Надежда“, Велико Търново	80
Pavlina Vladeva , 30 Years Club in Domestic Culture “Nadezda”, Veliko Tarnovo	80
Евгени Коев , Праисторическа керамика от проучванията в пещерите в района на гр. Велико Търново... 90	90
Evgeni Koev , Prehistoric Ceramics Found During the Research in the Caves in the Veliko Tarnovo Region.....	90
Евгени Коев , Пещерата „Утроба“ и скалният култов комплекс около нея в долното течение на река Осъм, Централна северна България.....	100
Evgeni Koev , The “Utroba” Cave and the Crown Cultural Complex Around It in the Lower Treatment of the Osam River, Central North Bulgaria.....	100
Паскал Пиперков , Идеи за поклоннически културни маршрути в Северен Централен район и в Северозападен район на България.....	116
Paskal Piperkov , Ideas for Cultural Routes for Pilgrimage in the North Central Region and the North West Region of Bulgaria	116
Михаела Кръстева , Предизвикателства в опазването, съхраняването и представянето на културно-историческо наследство.....	126
Mihaela Krasteva , Challenges in Protecting, Preserving and Presenting Cultural and Historical Heritage	126
Жолт Ласло Маркус, Тибор Скалицки, Габор Капоши, Миклош Вереш, Детелин Лучев , Индивидуален туристически аудио пътеводител GUIDE@HAND и приложения за български културни активи	142
Zsolt László Márkus, Tibor Szkaliczki, Gábor Kaposi, Miklós Veres, Detelin Luchev , Individual Travel Audio Guide GUIDE@HAND and Applications for Bulgarian Cultural Assets.....	142

Калина Сотирова-Вълкова, Институционализираното наследство в 21 век. Методология за дигитализация и е-битие..... 155

Kalina Sotirova-Valkova, Institutionalised Heritage in 21 Century. Digitalization Methodology and e-Being 155

Публикации по проект „Модели и концепции на сериозни образователни игри чрез свързани мултимедийни ресурси от военно-историческото наследство“ с номер на договор с фонд „Научни изследвания“ (ФНИ): ДМ 02/3 167

Publications under the Project “Models and Concepts of Serious Educational Games through Related Multimedia Resources of the Military-Historical Heritage” under the Contract Number with the Scientific Research Fund (NSF): DM 02/3 167

Галина Богданова, Николай Ноев, Защита на цифрови ресурси в областта на културното наследство в библиотеки, музеи, архиви и галерии в Северна и Централна България..... 168

Galina Bogdanova, Nikolay Noev, Protection of Digital Resources in the Field of Cultural Heritage in Libraries, Museums, Archives and Galleries in Northern and Central Bulgaria 168



ЗАЩИТА НА ЦИФРОВИ РЕСУРСИ В ОБЛАСТТА НА КУЛТУРНОТО НАСЛЕДСТВО В БИБЛИОТЕКИ, МУЗЕИ, АРХИВИ И ГАЛЕРИИ В СЕВЕРНА И ЦЕНТРАЛНА БЪЛГАРИЯ

Галина Богданова, Николай Ноев

*Институт по математика и информатика, Българска академия на
науките, София, България*

PROTECTION OF DIGITAL RESOURCES IN THE FIELD OF CULTURAL HERITAGE IN LIBRARIES, MUSEUMS, ARCHIVES AND GALLERIES IN NORTHERN AND CENTRAL BULGARIA

Galina Bogdanova, Nikolay Noev

*Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
Sofia, Bulgaria*

Abstract: *The article examines approaches and methods for marking and protecting digital resources in the field of cultural and historical heritage. Artifacts from cultural institutions (libraries, museums, archives and galleries from North and Central Bulgaria) are documented, digitized, indexed and organized in digital repositories. Technologies have been researched to protect some types of digital resources, organized in archives and repositories. A methodology has been developed to protect different levels and for different types of media - photo, audio, video, text.*

Keywords: *Digital Resources, Digital Archive, Digital Repository, Cultural Heritage, Metadata, Protection, Storage Organization*

Резюме: *В статията са разгледани подходи и методи за маркиране и защита на цифрови ресурси от областта на културно-историческото наследство. Артефакти от културни институции (библиотеки, музеи, архиви и галерии от Северна и Централна България) са документирани, цифровизирани, индексирани и организирани в дигитални хранилища. Проучени са технологии за защита на някои видове цифрови ресурси, организирани в архиви и хранилища. Разработена е методика за защита*

на различни нива и за различни типове медии - фото, аудио, видео, текст.

Ключови думи: Цифрови ресурси, Цифров архив, Дигитално хранилище, Културно наследство, Метаданни, Защита, Организация на данни

1. Въведение

Цифровите ресурси са неразделна част от представянето на знания в областта на културно-историческото наследство (КИН). Съвременните тенденции в това направление са съдържанието да се създава, съхранява, обработва и представя в цифров вид.

В настоящето проучване са разгледани подходи и методи за маркиране и защита на цифрови артефакти и единици от библиотеки, музеи, архиви и галерии. Разработена е методика за защита на дигиталните хранилища.

2. Методи за защита и влагане на криптирано съдържание в цифрови ресурси

Основен етап от създаването на цифрови ресурси е защитата на информацията в тях от неоторизирано разпространение. Изследванията в тази област са свързани с търсенето на ефективни методи за вграждане на знаци, серийни номера и др. в оригиналните данни, доказващи техния произход. Въвеждането на все повече рестриктивни мерки от страна на някои правителства върху криптиращите услуги мотивира търсенето на методи, чрез които да се скрие информация в оригиналните данни. Изследванията в тази област се развиват в няколко поддисциплини. Едни от най-важните от тях са криптографията от областта на теория на кодирането и стеганографията.

2.1. Стеганографски методи за вграждане на информация в цифровите данни

Стеганография в буквален превод от гръцки означава „тайнопис“. Както и останалите подобласти, занимаващи се със скриването на информация и стеганографията прикрива съобщението, което искаме да остане скрито. За разлика от други подобласти като криптографията например, които се занимават с прикриването на самото съобщение, стеганографията се опитва да прикрие факта, че въобще такова вградено съобщение съществува. Вграждането трябва да бъде извършено по такъв начин, че трета страна, имаща достъп до обекта, да е неспособна да засече наличието на тайнописа. В една „идеална“ система покриващият обект трябва да не може да бъде различен от стего обекта, нито от човек, нито чрез методи за статистическо компютърно търсене. Теоретично, покриващият обект би могъл да бъде всеки тип компютърно обработвани данни като статични изображения, видео, звук и текст.

Стеганографските методи за вграждане на информация използват излишните данни на цифров обект за да се запише тайна информация. И модификациите, направени при процеса на вграждане, трябва да бъдат незабележими за всеки неучастващ в комуникацията. Това налага необходимостта покриващият обект да съдържа достатъчно количество излишна информация, която да бъде заменена от секретните данни. Например всеки тип данни, които са резултат от някакъв вид физическо сканиране, съдържат стохастически компонент, наречен шум. Такива случайни изменения могат да бъдат използвани в процеса на тайна комуникация.

И стеганографията и защитата с воден знак имат за цел скрито пренасяне на информация. Въпреки това съществуват и съществени разлики между двата похвата. Стеганографията се отнася до скритата комуникация между две страни. По този начин стеганографските методи обикновено не са устойчиви на модификация на данните или имат ограничена устойчивост и защита на вградената информация срещу технически модификации, които могат да възникнат по време на предаване или съхраняване като конвертиране, компресия, трансформация на дигитален към аналогов сигнал.

Защитата с воден знак от друга страна притежава допълнителна устойчивост срещу опити да се премахне вградената информация. По този начин защитата с воден знак е приложима в случаите когато покриващият обект е достъпен до трети страни, които знаят за наличието на скрити данни в него и имат интерес от премахването на скритите данни. Едно от най-известните приложения на защитата с воден знак е доказване на авторски права върху дигитални данни, като се вгради скрита информация в тях. Друго приложение е следенето на разпространението на данни с цел събиране на данни от маркетингова гледна точка. Известни приложения са и добавяне на помощни данни към архив и подписване при опит за промяна на данните.

При стеганографията се прикрива самия факт на съществуване на тайното съобщение. Цифровата стеганография може да се раздели основно на четири направления:

- Вграждане на информация с цел скритото и предаване;
- Вграждане на цифров воден знак;
- Вграждане на идентификационни номера;
- Вграждане на заглавия.



Фигура 1. Влагане на скрити данни в мултимедия

2.2. Защита на цифрово съдържание с воден знак

Цифровият воден знак е видим или за предпочитане невидим идентификационен код, който е перманентно вграден в цифрови дан-

ни и запазва присъствието си в тях след извличане му. Той е специален знак, незабележимо вграден в изображение, текст или друг сигнал с цел да се осъществи контрол върху използването на този сигнал [1, 2, 3, 4, 5, 6, 7].

Всички методи за защита с воден знак имат едни и същи основни съставни блокове: система за вграждане на воден знак и система за извличане на воден знак. Входните данни към системата за вграждане са водния знак, покриващия обект и незадължителен публичен или таен ключ. Водният знак може да бъде от всякакъв тип като число, текст или изображение. Ключът се използва за да се предотврати неоторизираното извличане и манипулиране на водния знак. В комбинация с публичен или таен ключ, техниките за воден знак се отнасят към тайна или публична защита с воден знак. Изходът от схемата са данни, защитени с воден знак.

Методи за защита на текст и изображения с воден знак:

- Методи за скриване на информация в пространствената област;
- Воден знак с разпростиращ се спектър;
- Кодиране чрез отместване на редовете;
- Кодиране чрез отместване на думите;
- Характеристично кодиране.

За да бъде една система за воден знак устойчива на атаки е необходимо да се спазват основни изисквания посочени в следващата таблица:

Таблица 1. Изисквания за устойчивост на система за воден знак.

Изисквания	Описание
Незабележимост	Модификациите, предизвикани от вграждането на водния знак, трябва да бъдат под прага на забележимост. Това означава, че е необходим критерий, който да се използва не само при дизайн на водния знак, но и за определяне на предизвиканите промени. Заради необходимостта от такава незабележимост, отделните елементи, които биват модифицирани се променят с оптимално малко количество
Излишество	За да се осигури устойчивост въпреки малкото позволени промени, информацията съставлява водния знак трябва да бъде разпределена с излишество върху много елементи на покриващия обект за да се осигури глобална устойчивост т.е. информацията да може да бъде възстановена само по малки части от данните, защитени с воден знак

Изисквания	Описание
Ключове	Системите за воден знак използват един или повече криптографски сигурни ключове за да се гарантира сигурността срещу манипулиране или премахване на водния знак
Устойчивост	Идеалната система за воден знак трябва да бъде устойчива на всякакъв вид промени, породени от стандартна или злонамерена обработка на данните. Тъй като такава практическа система не е открита, се прави компромис между устойчивостта от една страна и незабележимостта и капацитета от друга. В зависимост от целта на конкретното приложение, желаната устойчивост повлиява на дизайна на водния знак. Например при воден знак, използван за изображения, ако искаме той да е устойчив на JPEG компресия с висок компресиращ фактор, е по-добре да използваме метод, който работи в трансформационната област, отколкото в пространствената. И обратно, ако искаме по-голяма устойчивост на геометрични трансформации като ротация, трансляция, мащабиране и т.н., е по-добре да използваме пространствената област

Тези принципи се отнасят до системи за воден знак, използващи всички видове данни като аудио, видео, форматиран текст и др.

Входните параметри към системата за извличане са данните, защитени с воден знак, таен или публичен ключ и в зависимост от метода за воден знак, оригиналните данни и оригиналния воден знак. Изходът е или извлечения воден знак W или някаква мярка за възможността водният знак, подаден на входа да присъства в разглежданите данни.

Системите за воден знак могат да бъдат разделени на три типа:

- Частен воден знак - такива системи изискват поне оригиналните данни. Системите от тип I извличат водния знак W от възможно променените данни и използват оригиналните данни за определяне дали водния знак присъства. Системите от тип II изискват също и копие от вградения воден знак и дават решение от тип „да” или „не” на въпроса: дали се съдържа водния знак;
- Получастен воден знак - не използват оригиналните данни за разпознаване, но дават отговор на същия въпрос;
- Публичен воден знак - това е проблематиката с най-много предизвикателства, тъй като в този случай не се изискват нито оригиналните данни, нито вградения воден знак.

2.3. Видове атаки срещу системи за воден знак

Според измененията, на които един воден знак би могъл да бъде подложен (преднамерено или непреднамерено) се различават две групи намеси. Първата включва намеси, които добавят някакъв допълнителен шум към данните, докато втората са модификации в пространствената област и геометрични промени, които целят да доведат до несъответствие между водния знак и ключът, използван при вграждане. Тези две групи атаки са известни като разрушителни атаки и синхронизиращи атаки. По-подробна класификация е направена в [1].

В зависимост от приложението и изискването на водния знак, списъкът на възможните атаки включва следните основни видове намеси:

- Промени в сигнала (промения в контраста, осветеността, цветови корекции, гама корекции);
- Адитивен и мултипликативен шум (Гаусов, равномерен и др.);
- Линеино филтриране (нискофестотно, високочестотно и др.);
- Нелинейно филтриране;
- Компресия със загуби (JPEG, H.261, H.263, MPEG-2, MPEG-4, MP3, MPEG-4, G.723);
- Локални и глобални афинни трансформации (транслация, ротация, мащабиране);
- Отрязване на данни (отрязване, хистограмни модификации);
- Смесване на данни (вмъкване на лого или кадър);
- Транскодиране (H.263 - MPEG-2, GIF - JPEG);
- Д/А и А/Д конвертиране;
- Множество водни знаци;
- Атака с колизии;
- Статистическо осредняване;
- Мозаечна атака.

2.4. Методи за защита на аудио файлове

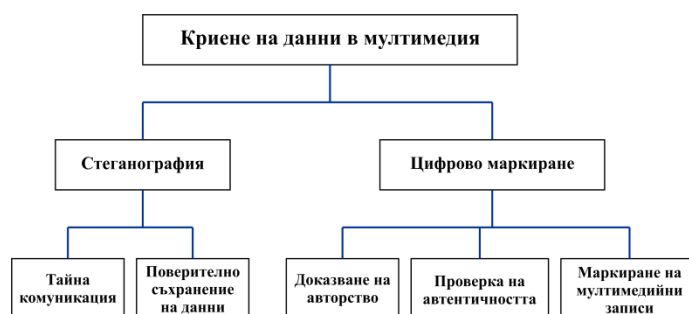
За вграждане на информация в аудио сигнали могат да се използват методи, приети при други видове стеганографии. Може да се вгради информация, замествайки най-малко значещите битове на основа на особеностите на аудио сигналите или на слуховата система на човека. Основните методи за защита на аудио файлове са изброени в следващата таблица:

Таблица 2. Методи за защита на аудио файлове.

Вид метод	Описание
Кодиране с разширяване на спектъра	Този алгоритъм удовлетворява повечето от поставените по горе изисквания. Цифров воден знак (ЦВЗ) се внедрява в аудио сигнала (последователност от 8- или 16- битова последователност), което води до незначително изменение на амплитудата. За отделяне на ЦВЗ не е необходим изходен аудио сигнал
Модификация на фазата на аудио сигнал	Вграждане на информация посредством модификация на фазата на сигнала е метод, при който фазата на началния сегмент на аудио сигнала се модифицира в зависимост от вгражданите данни. Фазата на следващите сегменти се съгласува с него за да се съхрани фазата. Това е необходимо, защото към разлики във фазата, човешкото ухо има по голяма чувствителност. Фазовото кодиране, когато то може да бъде приложено, се явява един от най-ефективните методи за кодиране, по критерий отношението сигнал-шум
Вграждане на информация за сметка на изменението на времето на задръжка на ехо-сигнал	Този метод позволява да се вгради информация в прикриващия сигнал, чрез изменение на параметрите на ехо сигнала. Параметрите на ехото, носещи вградената информация спадат: начална амплитуда, време за спад и време на задръжка между изходния сигнал и неговото ехо. При намаляване на това време на задръжка двата сигнала се смесват. В определена точка човешкото ухо престава да различава двата сигнала и ехото се възприема като добавен резонанс. Трудно е да се определи точно тази точка, тъй като тя зависи от изходния запис, типа на звука и слушателя
Маскиране на скритата информация	Методът с маскиране на сигнала използва ефект, при който слабо, но чуваемо звуково колебание става нечуваемо при наличие на друго по-силно звуково колебание (маскиращ сигнал). Ефектът на маскиране зависи от спектралната и времева характеристика на маскирания и маскиращия сигнал

2.5. Основни области на приложение на криене на данни в мултимедия

По отношение на мрежово-базираните сценарии (Интернет пространството) и приложения, съществуват пет основни приложни области на технологиите за криене на данни в мултимедия [1, 8, 9], които са показани на следващите фигура и таблица. Първите две приложни области попадат в рамките на научноизследователското направление стеганография, а останалите три са предмет на изследване на направлението цифрово маркиране.



Фигура 2. Области на приложение на криене на данни в мултимедия

Таблица 3. Области на приложение на криене на данни в мултимедия

Област на приложение	Описание
Стеганография	
Тайна комуникация	Разглежда предаването на поверителни съобщения през глобалната мрежа с помощта на цифрова мултимедия. Целта на тайната комуникация е подобна на предаването на криптирани данни – гарантиране на поверителността на личната комуникация между двама участници. Допълнителното предимство на стеганографските техники в тази област е, че те скриват самото наличие на комуникационен процес чрез вграждането на съобщенията в произволно мултимедийно съдържание. Двамата участници в комуникацията използват мултимедийни данни, чието съдържание е видимо за произволни трети лица (например снимки в Интернет блог) и не е поверително. Наличието и смисълът на тайните съобщения, вградени в мултимедията остават неоткриваеми от неупълномощени трети лица.

Област на приложение	Описание
Поверително съхранение на данни	Невидимо съхранение на поверителни данни като номера на кредитни карти, банкови сметки, пароли и др. Сигурността на съхранението на тези данни може да бъде повишена с помощта на технологиите за вграждане на данни в мултимедия. Те могат да направят криптираните лични данни невидими, като ги вградят в мултимедия. По този начин се повишава нивото на защита - добавя се допълнителен защитен слой (допълващ криптографската защита) между конфиденциалните данни и потенциалните хакери.
Цифрово маркиране	
Доказване на авторство	Засяга защитата на интелектуалната собственост и позволява доказване на авторски права върху дадена мултимедия. Технологиите за криене на данни могат да вградят информация за истинския автор директно в мултимедийното съдържание. По този начин, когато възникнат спорове, касаещи авторските права върху произведението, законният автор може да докаже и защити своите права.
Проверка на автентичността	Отнася се до защитата на мултимедийно съдържание срещу неправомерни промени. Посредством технологиите за криене на данни отделните региони от мултимедийното съдържание, които са били неправомерно променени, могат да бъдат разпознати и в зависимост от използвания метод, оригиналното съдържание може даже да се възстанови до определена степен.
Маркиране на мултимедийни записи	Засяга също защитата на авторски права. По подобие на приложенията за доказването на авторство, методите за криене на данни вграждат информация, която идентифицира купувача или законния ползвател на мултимедийното съдържание. По този начин, ако се предприемат действия, нарушаващи правата на автора – като например нелегално разпространение на мултимедийното съдържание в Интернет – нарушителят може да се разпознае посредством скритата информация, вградена в нелегално разпространените копия.

Представените пет приложни области описват само най-значимите и най-разпространените приложения на криенето на данни в мултимедия, които имат отношение към глобалната мрежа. Интернет е изключително динамична среда и този списък от приложения лесно може да се разшири с нови области на приложение при всеки по-важен етап на развитие и напредък на модерните информационни и комуникационни технологии.

3. Защита на цифрови ресурси с видим знак

Проучени са основните класове, понятия и критерии за оценка на сигурността на компютърните системи. Разгледани са четирите класа на сигурна защита (доказана сигурност, временна сигурност, разумна сигурност, минимална сигурност) и обобщените категории на

техните критерии (политика на сигурност, отчетност, гарантираност, документираност).

Документирани са артефакти от фондовете на участници в проекта като съдържанието им е дигитализирано, обработено и представено в цифров вид. По разгледаните подходи и методи за маркиране и защита на цифрови ресурси е разработена методика за защита на дигиталните хранилища на различни нива (фигура 3). За организиране на цифровите архиви е използвана софтуерната среда FotoStation на компанията FotoWare¹, специализирана за създаване на цифрови масиви, индексирание на медия файлове и организиране на дървовидна файлова структура. Софтуерната среда FotoStation има възможност за надграждане с клиент-сървър системата Cameleon за работа с много клиентски приложения и доставянето на файловете като интернет ресурси. Позволява и програмиране на допълнителни функционалности, които да автоматизират и обогатят обработването на цифровите ресурси.



Фигура 3. Защита с видим воден знак на изображение на Трапезица.

Разработено е приложение за защита на изображения с воден знак използващо описаните методи и техники: защита чрез воден знак

¹ FotoWare (FotoStation и Cameleon), <http://www.fotoware.com>

в пространствената област; допълнителна устойчивост чрез схемата RS код, вътрешен код; корекция на коефициента на устойчивост и гъстота на използваните битове; допълнителна парола – CRC на паролата се използва за инициализация на генератор на псевдослучайни числа, определящи позициите за вграждане. Анализирани и други методи за защита за защита на изображение с цифров воден знак като “uMark” [11] и други специализирани софтуерни продукти.

4. Заключение

Защитата на цифровите ресурси се превръща в необходима и задължителна стъпка при създаването на ново цифрово съдържание в областта на КИН.

Благодарности

Това изследване е частично подпомогнато по проект „Модели и концепции на сериозни образователни игри чрез свързани мултимедийни ресурси от военно-историческото наследство“, с номер на договор с фонд „Научни изследвания“ (ФНИ): ДМ 02/3.

Литература

1. Berger T., T. Todorov, Improving the Watermarking Process With Usage of Block Error-Correcting Codes, *Serdica Journal of Computing*, 2, 163-180, 2008
2. Bogdanova, G., Todorov, T., Noev, N. Effective methods for organization and presentation of digitized cultural heritage. *International Journal of Mechanical Engineering & Technology (IJMET)* - Scopus Indexed, 9, 4, Copyright ©IAEME, 2010, 2018, ISSN:Print: 0976 – 6340, Online: 0976 - 6359, 991-1000. SJR:0.21

3. Todorov, T., Bogdanova, G., Shatko, E., Noev, N. Digital repository of cultural heritage objects. *International Journal of Mechanical Engineering & Technology (IJMET)*, 9, 6, Copyright ©IAEME, 2010, 2018, ISSN:Print: 0976 – 6340, ISSN Online: 0976 - 6359, SJR:0.215
4. G. Bogdanova, N. Noev. Chapter 8: Digitization and Preservation of Digital Resources and Their Accessibility for Blind People. Book “Cyber-Physical Systems for Social Applications”, IGI Global, 2018
5. Bogdanova, G., Todorov, T., Georgieva-Tsaneva, G.. Software Approaches and Methods to Ensure the Security of Interactive Systems. *Cybernetics and Information Technologies*, 18, 5, Institute of Information and Communication Technologies - BAS, 2018, ISSN:1311-9702, 12-20. SJR:0.204
6. Bogdanova, G., T. Todorov, N. Noev. Creating and Representing Semantic Knowledge of Bell Objects. *International Journal of Applied Engineering Research*, 12, 19, Research India Publications, 2017, ISSN:0973-4562, 8986-8994. SJR:0.149
7. Bogdanova G., T. Todorov, N. Noev, Digitalization and security of “Bulgarian folklore heritage” archive, *Proc. 11th International Conference on Computer Systems and Technology*, 2010
8. Brassil J., S. Low, N. Maxemchuk, L. O.Gorman. Hiding information in document images, In *Proceeding of the 29th Annual Conference on Information Sciences and Systems*, 482-489, 1995
9. Cox I., J. Kilian, T. Leighton, G. Shamoon, Secure Spread Spectrum Watermarking for Multimedia, *IEEE Transactions on Image Processing*, 6(12), 1673-1687, 1997
10. Kutter M., Digital signature of color images using amplitude modulation, *J. Elec-tron. Imaging*, 326-332, 1998
11. uMark, <https://www.uconomix.com/Products/uMark/Default.aspx>

*Галина Богданова, Николай Ноев
Институт по математика и информатика, Българска академия на
науките, София, България*

*Galina Bogdanova, Nikolay Noev
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
1113 Sofia, Bulgaria, 8, Acad. G. Bonchev Str.
e-mail: g.bogdanova@gmail.com*

<i>Научна поредица</i>	<i>Science series</i>
<i>Културно-историческо наследство:</i>	<i>Cultural and Historical Heritage:</i>
<i>опазване, представяне,</i>	<i>Preservation, Presentation,</i>
<i>дигитализация</i>	<i>Digitalization</i>
<i>Том 4, брой 1, 2018</i>	<i>Volume 4, Issue 1, 2018</i>

<i>Редактори</i>	<i>Editors</i>
<i>Петко Ст. Петков</i>	<i>Petko St. Petkov</i>
<i>Галина Богданова</i>	<i>Galina Bogdanova</i>

<i>Институт по математика и</i>	<i>Institute of Mathematics and</i>
<i>информатика, БАН</i>	<i>Informatics, BAS</i>

<i>РНБ „П. Р. Славейков”</i>	<i>RPL “P. R. Slaveykov”</i>
<i>Велико Търново, България</i>	<i>Veliko Tarnovo, Bulgaria</i>

ISSN: 2367-8038
Web: <http://www.math.bas.bg/vt/kin/>