СТЕГАНОГРАФСКИ ПОДХОД ЗА СКРИВАНЕ НА ДАННИ В AVI ФАЙЛ*

СВЕТЛОМИР Ц. СПАСОВ, ХРИСТО И. ПАРАСКЕВОВ

STEGANOGRAPHY APPROACH TO HIDING DATA IN AVI FILE

SVETLOMIR TS. SPASOV, HRISTO I. PARASKEVOV

ABSTRACT: *This article describes a method for hiding text messages in multimedia uncompressed video file formats by using LSB algorithm in video streams of uncompressed video formats, preventing noticeable difference in the size and quality of the manipulated file from the original one.*

KEYWORDS: *Steganography in AVI, LSB, information security*

I. Въведение

С появата на компютрите и съвременните технологии стеганографията в взаимодействие с крипографията се превръщат във все по използвани методи за опазване на информация и заемат по-широка употреба в заобикалящия ни свят. Използвайки лесно достъпни и широко разпространени цифрови формати, като текстови, изображение, аудио- и видеофайлове за прикриване на информация. Виртуалното пространство достъпно от глобалната мрежа позната ни като „Интернет“ ни предоставя огромен обем от разнообразни социални средства за обмен на информация. Медийните файлове обикновено са големи по размер, позволявайки ни да прикрием в тях чрез софтуерна технология за манипулиране на информацията големи количества данни.

За да бъде сигурна комуникацията тя трябва да бъде незабелязана а за по-голяма сигурност и неразбираема. Само в такава комбинация съобщението ще бъде предадено сигурно до своя получател. В момента, в който сигурното послание се разкрие от недоброжелатели стеганографията се проваля, защото нещото, което е било предвидено да бъде скрито, е станало явно. И тази сигурност в криптографията позната ни като принципа Kerckhoff на холандцкия лингвист и криптограф е приложима за стеганографията гласи, че една криптосистема трябва да остане защитена дори и ако всичко свързано с нея е публично достояние [1].

Има много методи за скриване на данни в цифров вид чрез ползването на различни файлови формати. Основно научните разработки са насочени над изображения и аудиофайлове. По-малко са изследванията над видеофайлове [2]. Самите аудио видео файлове са по-непредпочитани за работа от гледна точка на сложната структура на файловете и голяма уязвимост от стегоатаки [3], но те са подходящи за това изследване защото са големи по обем, което позволява работа с над 1000 символа за вграждане и тази информация да остане невидима и трудна за намиране. А и факта, че са по-малко проучвани в областта на стеганографията е стимул за работа.

* Настоящата статия е финансирана от Фонд „Научни изследвания” към Шуменския университет „Епископ Константин Преславски“ по проект № РД-08-119/2016 г.

II. Избор на видео файлов формат за контейнер

Съществуват различни видео файлови формати. Преценката за избор на формат се свежда до удовлетворяване на следните изисквания:

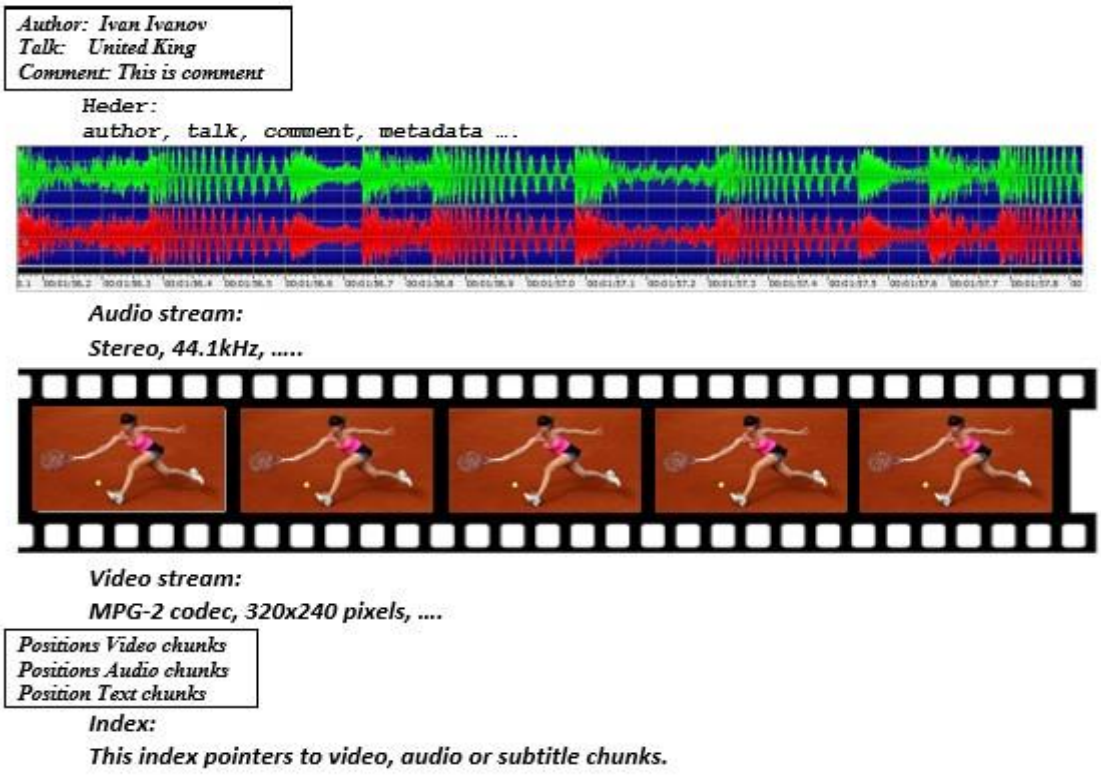
1. Скриване на голям по обем текст (над 1000 символа), който да бъде внедрен без видима разлика както в размера така и при възпроизвеждане на мултимедийния файл.

2. Простота на стеганографския алгоритъм, който ще позволи и по-бързото обработване на информацията, а оттам и изискванията за компютърната конфигурация ще бъдат по-малки.

Съчетанието на тези фактори е причина за избор на AVI видеофайл, който по структура на софтуерното си изграждане не се различава изключително много от останалите видео формати.

AVI известен още като Audio Video Interleave е мултимедиен контейнер формат въведен от Microsoft през 1992г. Структурата му се състои от обвивка (контейнер), в която са разположени синхронизирани аудио и видео потоци. AVI файла е изграден от обща файлова структура наречена Resource Interchange File Format. RIFF файловете са изградени от поредица парчета всяко от които е с големина 4 байта и съхранява индификационен номер. Неидентифицирани парчета в редицата могат да бъдат пропускани което позволява на файловия формат да бъде удължаван без да се повреждa.

Блокове мултимедийни файлове са в тялото на контейнера. Главата или позната още като header съдържа информация за целия AVI файл като например броя мултимедийни потоци, широчина и височина на файла и друга системна информация. В header и movie списъците се използват под парчета за техните данни. Списъка Index се намира в края на контейнера и съдържа в себе си информация с указатели към видео, аудио парчетата както и субтитър потоци ако са включени такива във файла [4].



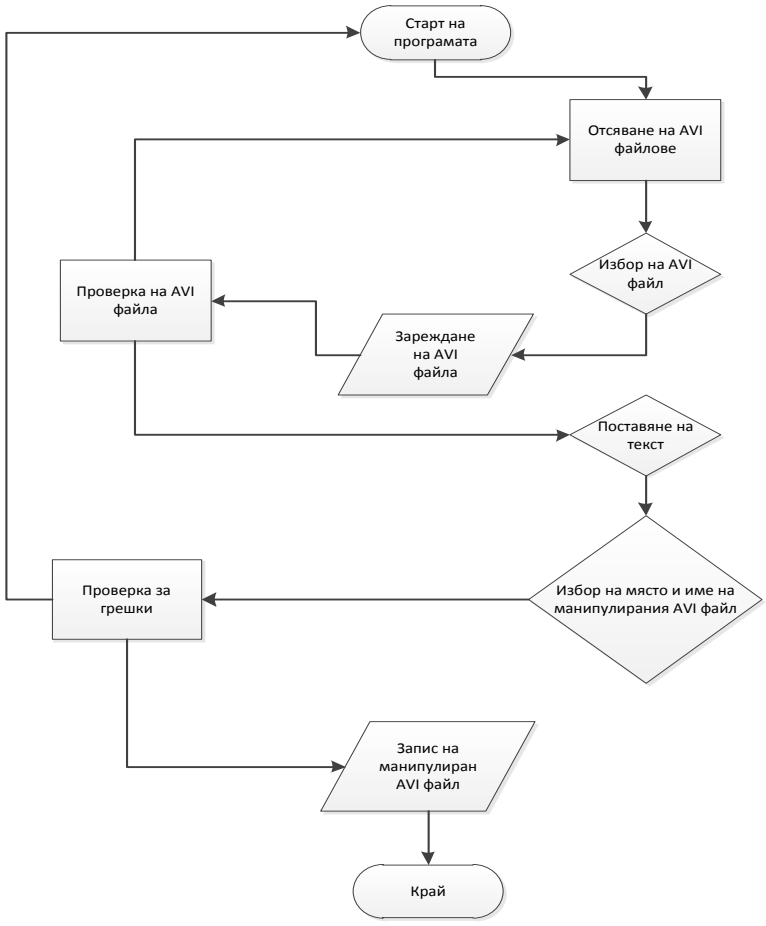
Фиг. 1 Визуално представяне на мултимедиен AVI файл

III. Алгоритъм за скриване на данни в AVI файл

Предложеният стеганографски алгоритъм се базира на LSB метода, като модифицира част от предоставените данни, съхранявани контейнера [5, 6]. Съществуват разработки, които успешно прилагат вграждането на скрита информация в аудиопотока, без това да причини звукова разлика при възпроизвеждането на файла. Предложеният алгоритъм използва видео потока от данни във AVI файла.

1. Вграждане на съобщение

- Проверка за съвместимост - алгоритъма не позволява зареждане на файл различен от AVI формат.
- Зареждане на AVI файла и проверка за броя фреймовете (frames), тъй като е поставено минимално изискване те да не са под 100.
- В първия фрейм се записва системна информация за дължината на съобщението. От втория фрейм нататък започва записването на съобщението като във всеки фрейм в началото заменя по 8 байта, като по този начин работи и с ASCII и с Unicode символни таблици позволявайки работата на програмата и на латиница и на кирилица.
- Запазване на стего файла.



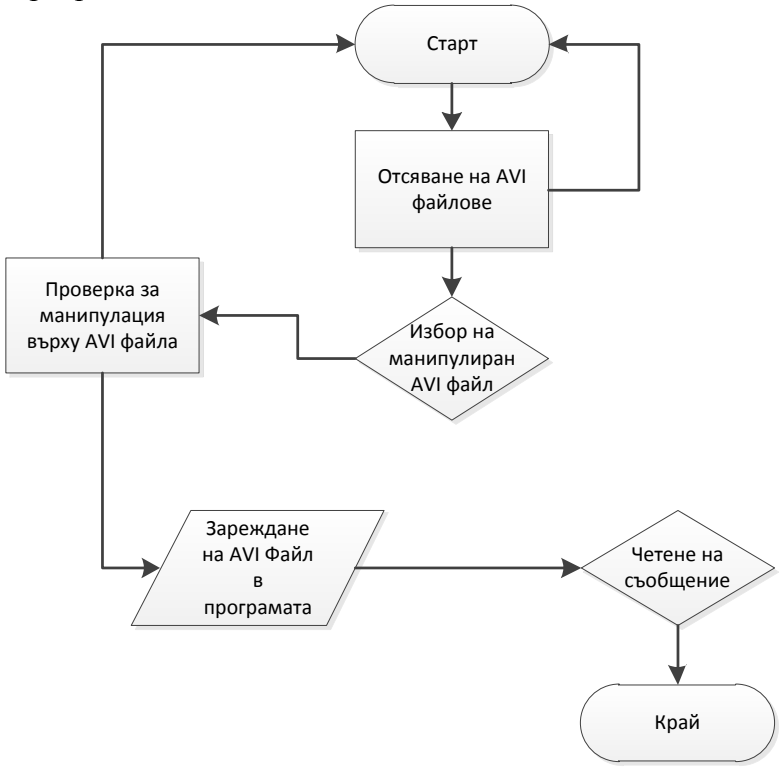
Фиг. 2 Вграждаща част от алгоритъма

2. Извличане на съобщение

- Зареждане на стего файла – описва се пътя до AVI файла

➢ Четене – програмата проверява за служебна информация в първия фрейм и ако намери такава вкарана с този алгоритъм то тя ще продължи да чете и ще възпроизведе в прозореца за съобщения скритото послание

➢ Изход от програмата



Фиг. 3 Извличаща част от алгоритъма

IV. Изисквания за софтуерната среда за разработване.

1. Обектно ориентирана среда с възможност за един и същи Java код, който да върви под различни операционни системи (така, че при евентуална минимална промяна да може да стартира на различни компютърни и преносими системи).
2. Да може да работи с мултимедийни файлове.
3. Приложението да бъде колкото е възможно по-малко като обем.
4. Да може да върви леко при обработване на големи по размер AVI мултимедийни файлове над 1GB., като процеса да бъде максимално съкратен от гледна точка на времетраене.

Избраната софтуерна среда за разработване на приложението е Eclipse Java Mars, която отговаря на горните изисквания.

V. Заключение

След проведените експерименти се установи, че софтуерната разработка на алгоритъма работи с различни по големина и резолюция AVI файлове. Постигнати са следните резултати:

➢ Скриване на текст в мултимедиен AVI формат.

➢ Липсва промяна в големината на файла, както и в качеството на видео- и аудио възпроизвеждането.

➢ Дължината на скритото съобщение зависи от броя на кадрите за секунда и продължителността на AVI видеофайла.

➢ Като направления за бъдещи изследвания по отношение на защита на скритото съобщение, могат да се посочат прилагане на разпръснато вграждане, използване на криптографски техники и други.

ЛИТЕРАТУРА

1. **D. Kahn.** The codebreakers: the story of secret writing/ Macmillan, 1967.
2. **J. Fridrich.** Steganography in Digital Media: Principles and Applications Cambridge University Press, 2010.
3. **E. Cole.** Hiding in Plain Sight: Steganography and the Art of Covert Communication. Wiley Publshing, Inc., 2003, Microsoft -2016г., София, България
4. URL:https://support.microsoft.com/bg-bg/contactus?forceorigin=esmc
5. URL:https://msdn.microsoft.com/en-us/library/windows/desktop/dd318189(v=vs.85).aspx
6. **N. F. Johnson, Z. Duric, and S. Jajodia.** Informaation Hiding: Steganography and Watermarking – Attacks and Countermeasures (Aduances in Information Security). Kluwer Academic Publishers, 2003