Latvijas Universitāte
Datorikas Fakultāte

Programmas «AtteluApstrade»
Modulis «Steganography»

programmatūras prasību specifikācija

Students: Andrejs Žmakins
Apl. nr. : az08189

Rīga 2010

Saturs

1. Ievads

1.1. Nolūks

Šī dokumenta nolūks ir precīzi specificēt programmas «AtteluApstrade» moduli «Steganography», lai identificēt visas prasības modulim un veidot pamatu programmatūras projektējumam.

Dokuments ir domāts gan pasūtītājam, gan izstrādātājam.

1.2. Produkta vīzija

LU MII izstrādātas programmas «AtteluApstrade» [sic] modulis «Steganography» domāts informācijas slēpšanai digitālajos attēlos.

Slēpjamo informāciju sauksim par ziņu (message), bet attēlu, kurā slēpsim ziņu – par konteineri (container). Ja konteinerā nav nekas nav paslēpts, tad saka ka konteiners ir tukšs. To pašu teiksim, ja pie ziņas nevaram tikt un to eksistenci nevaram pierādīt.

Ziņu uztversim kā bitu masīvu, līdz ar to ziņas garumu parasti izteiksim bitos.

Par slēpšanu sauksim tādu konteinera pārveidojumu, kā cilvēka uztverē tas vizuāli nemainās vai izmaiņas ir mazsvarīgas; bet pārveidojuma rezultātā pie dotas paroles (password) ziņa tiks iekodēta konteinerā.

No konteinera ziņu var izņemt ārā zinot paroli.

Ziņas spēju pārdzīvot konteinera izmaiņas pie attēlu apstrādes procedūrām, pārveidojumu formātā ar kompresiju ar zudumiem (lossy compression) sauksim par izturību (robustness). Ja ziņa spēj pārdzīvot relatīvi stiprākas izmaiņas, tad saka ka tai izturības pakāpe ir augstāka. (Acīmredzami, pie lielākas izturības pakāpes ziņas slēpšana stiprāk ietekmēs konteineri).

Iesaistīto pusi, kas tīšām vai netīšam mēģina iznīcināt ziņu konteinera, vai [tīšām] noteikt ziņas klātbūtni konteinerā sauksim par uzbrucēju (attacker). Ziņas iznīcināšanas mēģinājumu sauksim par uzbrukumu (attack).

Cita izturības definīcija: Izturība ir ziņas spēja pārdzīvot tādus uzbrukumus, kas stipri nemaina konteinera izskatu.

Moduļa funkcijas šajos terminos precīzas definēsim sekojoši:

1. Modulis «Steganography» nodrošina iespēju paslēpt konteinerī ziņu, norādot paroli un izturības pakāpi.
2. No konteinera izņemt tajā paslēpto ziņu, ja ir zināma attiecīgā parole.

2. Aktualitāte

Realizētām tehnoloģijām ir vairāki pielietojumi. Pirmais ir autortiesību pierādīšana. Žurnālists, pirms fotogrāfiju iesūtīšanas ziņu aģentūrai, var atzīmēt tos ar neredzamam ūdenszīmēm. Ja kāds nelikumīgi pasludinās tas par savējiem, krāpšana būs viegli pierādāmā. Otrkārt, var ar atšķirīgām ūdenszīmēm atzīmēt vairākas filma kopijas domātas vairākiem kinoteātriem un disku rakstīšanas rūpnīcām. Ja filma «noplūda» peer-to-peer tiklos, tad var izsekot no kurienes. Trešais iespējamais pielietojums ir Interneta cenzūras pārvarēšana. Steganogrāfija var būt viens posms drošā datu pārraides kanālā no totalitāra valsts. Moduļa funkcionalitātes lietošanas iespējas ir izsmeļoši aprakstītas sadaļā «Lietošanas scenāriji».

3. Vispārīgās prasības

1. Programmai jānodrošina divas paslēpšanas metodes:
    1. pirmajai metodei jābūt pēc iespējas ātrai un tai arī jānodrošina liels ziņas apjoms; izturība pret uzbrukumiem šai metodei nav svarīga;
    2. otrajai metodei jānodrošina regulējamo paslēptas informācijas izturības līmeni (ziņās apjoms nav vitāli svarīgs, kā arī ātrdarbība); izturību jānodrošina pret sekojošām izmaiņām:
        1. konversiju starp formātiem un saglabāšanu tajā pašā formātā;
        2. konversiju formātā ar mazāko krasu skaitu;
        3. konteineris ir konvertēts formātā, kas izmanto saspiešanu ar zudumiem (piemērām, JPEG);
        4. trokšņa pielikšana;
        5. izmēra mainīšana;
        6. kādas konteinera daļas zaudējums: ja konteiners ir apgriezts no malas un/vai konteinera iekšienē kaut kas ir aizkrāsots (teiksim, bildei virsū «uzzīmēts» teksts);
        7. konteinera pikseļu nobīde;
        8. konteinera pagrieziens par patvaļīgo leņķi;
        9. spožuma un kontrasta regulējums;
        10. aizmiglojums (blur);
        11. krāšu komponenšu (RGB) intensitātes regulējums;
        12. pārveidojumu uz melnbalto;
        13. uzasinājums (sharpen).
2. Katrai metodei jābūt iespējai šifrēt informāciju ar šifru ar 64-bitu garu atslēgu.

4. Funkcionālas prasības

Paslēpt konteinerā ziņu ar ātro neizturīgo metodi.

Ievade: tukšs konteineris, ziņa, parole.

Izvade: konteineris ar paslēpto ziņu.

Kļūda: Ziņa pārāk gara tādam konteinerim. Saīsiniet ziņu var izvēlējieties lielāko konteineri.

Paslēpt konteinerā ziņu ar izturīgo metodi.

Ievade: tukšs konteineris, ziņa, parole, izturības pakāpe procentos.

Izvade: konteineris ar paslēpto ziņu.

Kļūda: Ziņa pārāk gara tādam konteinerim. Saīsiniet ziņu var izvēlējieties lielāko konteineri.

Pārbaudīt vai konteinerā ir ziņa paslēpta ar ātro neizturīgo metodi.

Ievade: konteineris, parole

Izvade: varbūtība (procentos) ar kuru konteinerī ir paslēpta ziņa ar ātro neizturīgo metodi.

Kļūda: Konteineris nav izvēlēts. Izvēlējieties konteineri.

Pārbaudīt vai konteinerā ir ziņa paslēpta ar izturīgo metodi.

Ievade: konteineris, parole

Izvade: varbūtība (procentos) ar kuru konteinerī ir paslēpta ziņa ar izturīgo metodi.

Kļūda: Konteineris nav izvēlēts. Izvēlējieties konteineri.

Nolasīt ziņu, kas paslēpta ar ātro neizturīgo metodi.

Ievade: Netukšs konteineris, parole.

Izvade: Ziņa.

Kļūda: Ziņu nevar izņemt. Vai nu ziņas nav, vai nu parole nav pareiza, vai nu ziņa ir stipri bojāta. Ja domājat kā problēma ir ar paroli, varat pamēģināt vēlreiz.

Nolasīt ziņu, kas paslēpta ar izturīgo metodi.

Ievade: Netukšs konteineris, parole.

Izvade: Ziņa.

Kļūda: Ziņu nevar izņemt. Vai nu ziņas nav, vai nu parole nav pareiza, vai nu ziņa ir stipri bojāta. Ja domājat kā problēma ir ar paroli, varat pamēģināt vēlreiz.

5. Prasības lietotāja saskarne

Lietotāja saskarnei jāpiedāvā sekojošas iespējas, informāciju konteinera slēpjot:

- izvēlēties ziņu (norādīt datni vai ievadīt tekstu);
- izvēlēties paslēpšanas metodi;
- norādīt slēpjamās informācijas izturības pakāpi;
- ievadīt paroli;
- novērtēt, cik pie dota slēpjamas informācijas apjoma (un izturības), izmainīsies konteiners (subjektīvs novērtējums; nepamānāmi, maz, stipri, tā ka paliek tikai troksnis utt.);
- cik daudz informācijas (bitos un baitos) var paslēpt pie dotām konteineri un izturības pakāpi;
- pārējo funkcionalitāti: konteinera izvēli, atvēršanu, apskati, saglabāšanu nodrošina programma «AtteluApstrade».

Un izņemot ārā no konteinera:

- ievadīt paroli;
- [iepriekš apskatīt ziņu;]
- saglabāt ziņu datnē (vajag norādīt faila vārdu un ceļu);
- [novērtēt paslēptas informācijas veselīgumu;]
- pateikt ka konteiners ir tukšs.

6. Nefunkcionālas prasības

6.1. Prasības izpildes videi

Programma tik(s/a) testēta uz Java VM versijas 1.6.0_20, kas strādā zem Windows XP SP3 (32-bit), un Fedora Linux 12 64-bit.

6.2. Prasības ātrdarbība

Programmai jāiekodē 100000 bitu garo ziņu 10 sekunžu laikā ar ātro neizturīgo metodi un 50 sekunžu laikā ar izturīgo. Atkarība starp ziņas garumu un iekodēšanas laiku abos gadījumos ir lineāra.

7. Mijējdarbība ar «AtteluApstrade»

Modulis izmanto sekojošus programmas «AtteluApstrade» objektus:

Util.RasterImage – operācijām ar konteineri,

gui.MFAListener.parentFrame – kā vecāko (parent) saviem logiem.

8. Lietošanas scenāriji

8.1. Autortiesību aizsardzība

Reportierim veicās nofotografēt kādu «kārsto» notikumu. Viņam gribās to nopublicēt internetā, lai foto būtu visiem redzams, tajā skaitā lai piedāvātu to ziņu aģentūrām nopublicēt par maksu. Bet jebkurš var lejuplādēt foto un teikt, ka notikumu nofotografēja viņš. Kvalitātes samazināšana, necaurspīdīgs un puscaurspīdīgs teksts uz bildes var būt nepietiekams – fotogrāfiju no malas var apgriezt, puscaurspīdīgo ūdenszīmi var restaurēt. Bet ja autors atzīmēs savu fotogrāfiju ar neredzamo ūdenszīmi, potenciālam autortiesību pārkāpējam par to nebūs ne jausmas. Bet ja tomēr viņš par to uzzinās, vienīgs veids no tā garantēti izvairīties būs stipra fotogrāfijas izkropļošana. Tād īstajām autoram būs labs pieradījums tiesas prāvā.

8.2. Aizsargātas informācijas noplūdes avota noteikšana

Kāda kompānija publicē datorspēli. Spēles diska kopijas nosūtītas vairākām disku rakstīšanas rūpnīcām. Netālu no oficiāla pārdošanas sakuma datorspēle noplūdusi failu apmaiņas tīklos, kas var nelabvēlīgi ietekmēt pārdošanu. Lai noteikt no kādas rūpnīcas notika noplūde, var katrai rūpnīcai iesūtīt diska kopiju ar spēles resursiem (tas bieži ir attēli), kas ir atzīmētas ar unikālajiem ūdenszīmēm. Labums šeit ir tāds, ka noplūdes avotu var noteikt, ja parādījās ne paša spēle, bet pat neautorizētas ekrānkopijas, kas liecina par noplūdi.

8.3. Cenzūras pārvarēšana

Kādā totalitārā valstī disidentu grupa cīnās par cilvēktiesību ievērošanu. Šī valsts ir stipra interneta cenzūra. Disidentu grupai jākontaktē ar līdzjutējiem citās (brīvākajās) valstīs. Īpaši ātri jāpārraida ziņas, ka valdība uzsāka represijas pret oponentiem. Var iepriekš norunāt, ka šīs nelaimes gadījumā kāds mazsvarīgs (lai nepievērstu lielas uzmanības) organizācijas biedrs nopublicēs sludinājumu par noteiktas lietas pārdošanu kādā starptautiskajā sludinājumu sarakstā. Fotogrāfijās, kas nāk kopā ar sludinājumu var ievietot ziņu ar svarīgo informāciju. Organizācijas līdzjutējiem paliek tikai novērot vai neparādījās ziņas par norunātas preces pārdošanu. Tas fakts, kā viens no organizācijas biedriem kaut ko pārdod visticamāk paliks nepamanīts ar valsts drošības dienestiem pietiekami ilgu laiku, lai pārraidīt ziņu. Sludinājumu saraksta vietā bildes pārraidei var izmantot peer-to-peer tīklus.

9. Atsauces