ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКИЦИЯЛАРНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ
МУХАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ

МАЪРУЗАЛАР МАТНИ

Фан: Стегонография алгоритмлари

Фан тури: Амалий

Йўналиш: 5330300- Ахборот хавфсизлиги (ахборот коммуникацияси технологиялари ва сервис)

ФАРҒОНА - 2018

Ушбу маъруза матни таянч университетнинг ишчи ўқув дастури асосида тайёрланган.

Тузувчилар:
АТТ кафедраси ассистенти **У.Худойназаров**

Тақризчилар:
Телекоммуникация инж.
кафедраси доценти **Н.Умаралиев**

«**ТАСДИҚЛАНГАН**»
ТАТУ Фарғона Филиали Кенгашининг
2018 йил 29 августдаги йиғилиши
№ _____баённомаси
Ўқув ва тарбиявий ишлар
бўйича директор ўринбосари
_____ А.Расулов

«Маъқулланган»
Ахборот-таълим технологиялари кафедраси йиғилишининг 2018 йил 27 августдаги 1-сонли баённомаси.

Кафедра мудири _____ С.М.Абдурахмонов

«Маъқулланган»
“Телекоммуникация технологиялари ва касбий таълим” факультети ўқув-услубий Кенгашининг 2018 йил 27 августдаги 1-сонли баённомаси

Кенгаш раиси: _____ О.Қўлдошев

«Тавсия этилган»
Ўқув-услубий бўлим бошлиғи _____ Ш.Умаров
2018 й “____”_____

1-маъруза

Фанга кириш

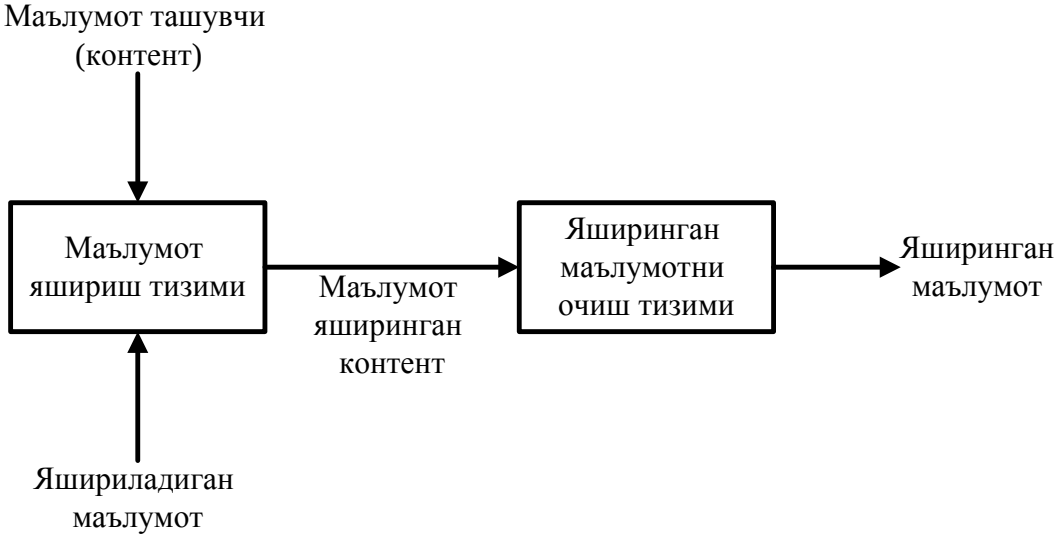
Режа:

1. Маълумотларни яшириш.
2. Стеганография ва watermarking (сув шаклидаги белги).
3. Уларнинг тарихи.
4. Стенография ва watermarkingнинг муҳимлиги.

Таянч иборалар: ахборотни яшириш, контент, watermarking, стегонография, муаллифлик ҳуқуқи.

1.1. Маълумотларни яшириш

Маълумотларни яшириш (information hiding ёки data hiding) қадимдан фойдаланилиб келинган ва долзарб бўлган соҳа саналган. Маълумотларни яшириш деганда контент (расмлар, қўшиқлар, видеолар ва ҳак.) ичида керакли маълумотларни яшириш тушунилади. Бу ерда, яшириш тушунчаси, маълумотни сезилмайдиган кўринишда келтириш ёки маълумот махфийлигининг мавжудлигини сақлаш учун фойдаланилади. Қадимда турли маълумотларни яшириш усулларидан фойдаланилган ҳолда, маълум доирадаги одамлар орасида маълумотлар алмашинилган. Умумий ҳолда маълумотлари яшириш тузулмаси қуйидагича:



1.1-расм. Маълумот яширишнинг умумий тузилмаси

Юқоридаги расмда кўрсатилганидек, тузилма икки қисмдан иборат: маълумотни яшириш (embedder) ва яширинган маълумотни очиш (Detector).

Маълумотни яшириш тизими иккита киришга, яшириладиган маълумот ва ушбу маълумотни ташувчи маълумот (контент) эга. Натижада эса, ягона маълумот яширинган контент ҳосил қилинади. Яширинган маълумотни очиш тизими эса битта киришга эга бўлиб, маълумот яширинган контентни қабул қилади ва ундан яширинган маълумотни ажратиб олади.

Одатда маълумотларни яшириш соҳаси иккита катта қисмга ажратилади:

- Стеганография;
- Watermarking (сув шаклидаги белги).

1.2. Стеганография ва watermarking (сув шаклидаги белги)

Watermarking. Бу тушунчани аниқроқ англаш учун қуйидаги мисолни келтирамиз. Америкaнинг 20 $ пулини олиб, ёриққа тутиб, президент Эндрю Джексон расмига қаралса, унда сиз ўнг томонда ушбу расмни билинар-билинмас (watermark) қилиб акланганини кўришингиз мумкин. Ушбу watermark қоғозни таёрлаш жараёнида унга қўшилган ва шунинг учун уни қалбакилаштириш мураккаб.

1.2-расм. Америкaнинг 20 $ пули

Ушбу келтирилган мисолга таяниб, **watermark** қуйидаги иккита хусусиятга эга. Биринчиси, watermark одатий кўриш жараёни орқали кўринишдан яширинган, яъни махсус кўриш жараёни орқали уни кўриш мумкин (масалан, ёриқликка тутиш орқали). Иккинчиси эса, watermark ўзи яширинган контентга тегишли маълумотни сақлайди (масалан, пулни қалбаки эмаслигини).

Бундан ташқари, watermarkларни физик объектлар ва электрон маълумотларга (мусиқа, расмлар ва видеолар) нисбатан ҳам қўлласа бўлади.

1990 йилларнинг охирларида келиб, рақамли тизимларда watermark тизимларига бўлган қизиқиш кучайди. Дастлаб асосий контент сифатида расмлар, аудио ва видео маълумотлари олинган бўлса, кейинчалик, бинар расмлар, матн, чизиқлар, анимацион параметрлар, юкланувчи кодлар ва ҳак. лардан ҳам фойдаланила бошланди.

Стеганография. Маълумот яширишнинг ушбу соҳасида, яширинган маълумот контентга ҳеч қандай алоқаси бўлмай, контент фақатгина маълумотни яшириш учун фойдаланилади. Масалан, фараз қилайлик Алиса махфий агент саналиб, у ўз шеригига махфий маълумотни юбормоқчи. Бунинг учун у, яқинда ўтган ёзги таътил тафсилотларини қоғоз мактубда тасвирлайди. Шундан сўнг, у сиёх рангини сутга алмаштиради. Шундан сўнг, одатий сиёх ранги билан ёзилган қаторлар орасига, махфий маълумотни ёзади. Сут қуригандан сўнг, қоғоздаги махфий маълумотлар оддий инсон кўзи учун кўринмас ҳолда ўтиб қолади. Ушбу мактубни, чироққа тутиб қаралса, махфий маълумотларни кўриш имконияти мавжуд бўлади. Watermarkдан фарқли равишда махфий маълумотлар, контентга тегишли эмас. У шунчаки махфий маълумотни яшириш учун фойдаланилган.

Стеганографияга бўлган талаб, 2001 йил 11 сентябр кунидаги воқеадан сўнг кескин ортди.

1.3. Уларнинг тарихи

Watermarking тарихи. Қоғоз хитойда 1000 йил аввал олдин ихтиро қилинган бўлиб, дастлабки қоғозлардаги белгилар, қоғозни қайси ташкилот томонидан ишлаб чиқилганини билдирган.

XVIII асрга белиб, европа ва америка қиталарида watermark турли ҳужжат ва пулларни қалбакилаштиришга қарши фойдаланилган.

Watermark атамаси 18 аср охирисида немис атамаси “wassermarke” келиб чиққан бўлиши тахмин қилинади. Watermark атамаси албатта нотўғри талқин этилган, яъни, белги яратилишида албатта сувни аҳамияти муҳим эмас. У қоғозга сув шаклидаги белги туширилганлиги сабабли, келиб чиққан.

Шундан сўнг, бу соҳада қатор ишлар қилинди. Маълумотни яшириш хусусида 1499 йилда аноним тарзда чоп этилган ҳикояга кўра, “Hypnerotomachia Poliphili” китобидаги ҳар бир бўлимларнинг биринчи ҳарфлари олинган ва “Poliam Frater Franciscus Columna Peramavit.” кетма-кетлик ҳосил қилинган ва унда “Father Francesco Columna loves Polia.” маълумоти ҳосил қилинган.

Шундан тўрт юз йил ўтгандан сўнг, дастлабки технология ёрдамида ҳосил қилинган watermark тизими яратилди. 1954 йилда Emil Hembrooke (Muzak Corporation) мусиқа ортида маълумот яшириш амалга оширилди. Бунда мусиқа орасида доимий такрорланувчи кичик узунликдаги бўшлиқлар қолдирилди. Ушбу бўшлиқлар узунликларига кўра “нуқта” ёки “тире” эканлиги аниқланади. Бунда Морзе колдаш усулидан фойдаланилган.

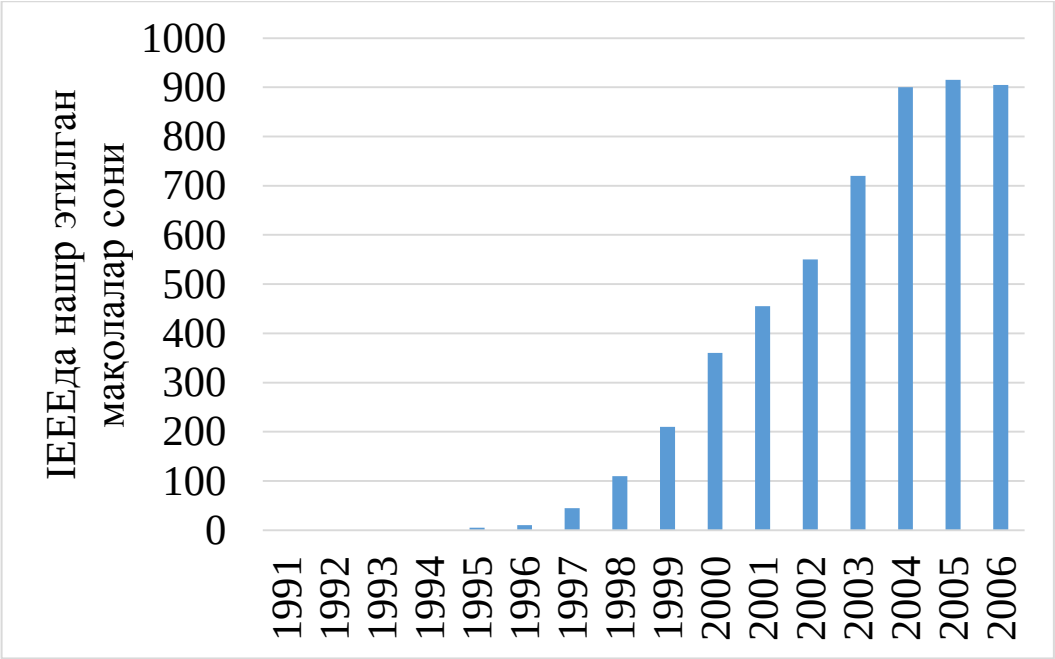
Шундан сўнг кўплаб ташкилотлар томонидан, watermarking технологияси турли стандартлар учун ишлатила бошланди. Copy Protection Technical Working Group (CPTWG) ташкилоти watermarking технологиясидан DVD ларда видеоларни ҳимоялашда фойдаланган бўлса, Secure Digital Music Initiative (SDMI) ташкилоти томонидан мусиқани ҳимоялаш учун фойдаланилди. Европанинг таниқли иккита ташкилоти, VIVA ва Talisman томонидан watermarking технологияси оммавий ахборот воситалари учун ишлатила бошланди.

Стеганография тарихи. Стеганография ҳақидаги дастлабки маълумотлар Геродот ҳикояларида учрайди (ундаги қуллар ва уларнинг сошсиз бошлари ҳақидаги ҳикоя). Бундан ташқари унинг “Demeratus” номли ҳикоясида, Спартани Греция томонидан режалаштирилган ҳужумдан огоҳлантирган Demeratus номли шахс, мумланган дарахт пўстлоғига маълумот ёзиб, устини яна бир маратоба мумлаган ва янги мумланган пўстлоғ сифатида ёнида сақлаб манзилга этказган.

Эней (қадимги Троя саркардаларидан бири) ўз даврида аёлларнинг қулоқ зираклари ёки шляпалар ёрдамида маълумотларни яшариш усулларидан фойдаланган.

Тилга асосланган стеганография энг қадимги усуллардан бири саналиб, махфий маълумотлар матндаги ҳар бир гапнинг биринчи ҳарфлари орқали ифодаланган. Ушбу усулнинг шакллантирилган шакли, Cardan томонидан ўрганилиб чиқилди. Бунга кўра яширинган маълумотни контент ичидан топишда махсус “маскалар”дан фойдаланилади. Маскалар ҳақидаги маълумот эса фақат икки томонгагина маълум бўлади. Ушбу усулдан биринчи жахон урушида немис ва антинемис кучларида кенг фойдаланилган.

Замонавий стеганография технологияси кўринишларидан бири Брассил ва бошқалар томонидан яратилди. Унга кўра, матндаги ҳарфларни ёки сўзларни 1/300 инчга юқорига ёки пастга сурилишини инсон кўзи англай олмайди. Аммо, махсус ксерикопия орқали уни аниқлаш жуда ҳам осон.



1.3-расм. Watermarking ва Стеганография бўйича чоп этилган моқолаларнинг йиллар кесимида кўриниши

1.4. Стенография ва watermarkingнинг муҳимлиги

Watermarking технологиясининг жадал ривожланиши асосан унинг муаллифлик ҳуқуқини таъминлаш (copyright protection)да фойдаланилиши сабаб бўлди. Интернет тармоғининг жадал ривожланиши, у орқали маълумот алмашинишининг ортиши, расм, мусиқа ва видео кўринишидаги маълумотларни кўчирилиши ва юкланиши, ўз навбатида муаллифлик ҳуқуқини таъминлаш муаммосини келтириб чиқарди.

Дастлабки маълумотлар аналог шаклда ёзилган бўлиб, унда бу муаммо унча сезилмаган. Сабаби, анаолог маълумотдан қайта-қайта кўчирилиши натижасида маълумот сифати камайиб боради. Аммо, рақамли шаклда маълумотларни ёзиш имкони натижасида, кўчирилган ва асл маълумот орасида сезиларли фарқ бўлмайди. Бу эса, маълумотларни қалбакилаштириш, муаллифлик ҳуқуқини бузулишига олиб келди.

Маълумот ҳимоясининг дастлабки усулларидан бири бу – криптография саналади. Криптография рақамли маълумот ҳимоясини таъминлашда кенг фойдаланилаётган усулдир. Криптографияда, хабар жўнатувчи маълумотни махфий калит билан шифрлайди ва шифрланган маълумотни интернет тармоғи орқали юборади. Қабул қилувчи, шифрланган маълумотни махфий калит билан дешифрлайди ва маълумотга эга бўлади. Аммо, криптографияда махсулот сотувчи ўз махсулотларини дешифрлангандан кейин мониторинг қилиш имкониятига эга бўлмайди. Масалан, сотув олувчи қонуний маълумотни сотиб олади ва калит билан уни дешифрлайди. Шундан сўнг, очиқ матнга эга бўлади ва уни ноқонуний

тарзда сотиш имкониятига эга бўлади. Бошқа сўз билан айтганда, криптография маълумотларни алмашиниш жараёнида хавфсизлигини таъминлай олади.

Бунинг натижасида, маълумотни дешифрлангандан сўнг ҳам уни ҳимоясини таъминлаш муаммоси долзарб бўлиб қолди. Watermarking технологиясида контент ичида жойлаштирилган watermark одатий фойдалинганда, шифрланганда, дешифрланганда, рақамли – аналог алмаштиришда, сиқиш жараёнларида ўчиб кетмайди.

Ҳозирда watermarking технологиясидан қурилмалар ва дастурий маҳсулотларни ноқонуний тарзда фойдаланишлардан ҳимоялашда кенг фойдаланилмоқда.

Электрон маълумот алмашиниши ортиши натижасида уларни ноқонуний тарзда қўлга киритиш, ўртада туриб эшитиш ёки маълумотни ушлаб қолиш каби таҳдидлар кенг тарқалди. Ушбу таҳдидларга қарши криптографиядан кенг фойдаланилсада, криптография технологиясида катта ҳисоблашлар ва математик амалларни бажариш талаб этилади.

Стеганографияда эса очиқ маълумот орқасида махфий маълумотни яшириш содда ҳисоблашни талаб этади. Бу эса бу технологияни исталган жойда фойдаланиш имконини беради.

Назорат саволлари

1. Маълумотларни яшириш ва уларнинг турлари.
2. Маълумотларни яшириш тузулмаси.
3. Стенография ва watermarking тарихи ва уларнинг муҳимлиги.

Фойдаланилган адабиётлар

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, (2008). Digital Watermarking and Steganography, the Morgan Kaufmann Series in Multimedia Information and Systems, 2nd Ed.
2. Peter Wayner, (2008). Disappearing Cryptography, Second Edition - Information Hiding: Steganography and Watermarking, Morgan Kaufmann.
3. Bruce Schneier, (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C, second Edition, John Wiley & Sons.

2-маъруза

Стенография ва watermarking иловалари

Режа:

1. Оммавий ахборот воситалари мониторинги.
2. Эгалик идентификацияси, эгалик тасдиғи, келишувларни аниқлаш.
3. Контент аутентификацияси, кўчиришни назоратлаш.
4. Қурилмаларни назоратлаш, стегонаграфия иловалари.

Таянч иборалар: Мониторинг, идентификация, келишувларни аниқлаш, контент аутентификацияси, кўчиришдан назоратлаш, иловалар.

1.1. Оммавий ахборот воситалари мониторинги

Watermarking жуда ҳам кўп иловаларда фойдаланилади. Умумий ҳолда бирор бир контент билан боғлиқ бўлган маълумот watermark сифатида қўйилади. Бу вазифани амалга оширувчи бошқа усуллар ҳам мавжуд. Масалан, бар кодлардан фойдаланиш, матн бошига сарлавҳа қўйиш ёки аудио ёзув бошида махсус таништирув сўзини қўйиш ва бошқалар. Шулардан келиб чиқиб қуйидагича савол туғулиши тайин. Watermarkingдан қайси ҳолларда фойдаланиш мақул ва содда усуллар бажара олмайдиган қандан имкониятларга эга ?

Watermarking бошқа усуллардан қуйидаги учта хусусияти билан ажралиб туради. *Биринчидан,* watermarking кўзга кўринмас. Бар кодлардан фарқли ўлароқ, расмлар турли-туманлигидан фойдаланмайди. *Иккинчидан*, watermarking ўзи жойлашган контентдан ажралмасдир. Матн бошига қўйилган сарлавҳалардан фарқли ўлароқ, улар қайта ишланиш давомида ўчириб ташланмайди ёки бошқа форматда ўзгартирилганда ўз ифодасини йўқотмайди. *Учинчидан,* watermarkingлар контент билан бир хил ўзгаришларни амалга оширишга қодирлиги, яъни баъзида, натижавий watermarkingга қараш орқали ундаги амалга оширилган ўзгаришлар ҳақида маълумот олиш мумкин. Ушбу хусусиятлар watermarkingни иловаларда кенг фойдаланишга асос бўлади.

Watermarking тизимларининг тўғри ишлаши бир нечта кичик хусусиятларга асосланади. Масалан, *чидамлилик* хусусияти watermarking тизими қандай даражада сигналлар устида тўғри амаллар бажарашини белгиласа, *ишончлилик* хусусияти эса watermarkingни қанчалик даражада яширинганлик даражасини белгилайди.

Стегонография эса юқоридаги усуллардан алоқанинг яширинганлиги билан фарқланади (масалан, алоқа фақат икки томон орасида маълум бўлиб, қолганлардан яширилади). Криптографияда эса махфийлик таъминланиб, шифрланган маълумот барчага маълум бўлади. Бутун алоқани яширишда эса стегонография зарур бўлади.

Стегонографик тизимларни тўғри ишлаши бир нечта хусусиятларга асосланади. Энг муҳуми, *статистик фош эта олинмаслик* хусусияти, контент таркибида яширинилган маълумотни очиш қийинчилигини кўрсатади. Бу билан боғлиқ бўлган яна бир хусусият бу – *стеганографик қобилят* саналиб, контентга кўпи билан қанча миқдордаги маълумотни яшириш имконияти билан белгиланади. Ҳар бир иловаларда яшириниладиган маълумот ҳажми турлича бўлади. Энг кичик яшириниладиган маълумот ҳажми 20 битни ташкил этиб, бу ҳолда бузғунчи томонидан уни аниқлаш имконияти мумкин бўлмайди. Ҳозирда имкони борича яшириниладиган маълумотни ҳажмини ошириш усуллари бўйича стеганографик тадқиқотлар олиб борилмоқда.

Watermarking кўплаб иловаларда фойдаланилиб, қуйида энг кенг тарқалган 7 та watermarking иловалари билан танишиб чиқалади.

Оммавий ахборот воситалари мониторинги. 1997 Японияда телевизион станцияларида реклама билан муаммо пайдо бўлган. Камида иккита телевизион станциясида кўрсатувлар вақтида доимий тартибсизликлар бўлган (бир телекўрсатув ўрнида бошқа телекўрсатув (реклама) қўйилган). Реклама берувчилар кўрсатилмаган рекламалари учун ҳам пул тўлашган. Ўша пайтда оммавий ахборот воситалари мониторинги мавжуд эмаслиги натижасида, ушбу муаммо 20 йил давомида аниқланмай қолаверган.

Кўплаб ташкилот ва шахслар томонидан оммавий ахборот воситалари (ОАВ) мониторингига қизиқиш ортди. Дастлаб ОАВ мониторинги технологияга асосланмаган бўлиб, унда инсон иштирок этган. Ушбу усулда ОАВ инсон ёрдамида кузатилиб борилган. Бу усул қиммат ва шунинг билан бирга хатолик даражаси юқори бўлган. Шуни ҳисобга олган ҳолда ОАВ ни техник мониторинглаш амалга оширила бошланди. ОАВ техник мониторинги икки усул асосида амалга оширилади:

- пассив мониторинг;
- актив мониторинг.

Пассив мониторингда тизимлари ОАВги контентни тўғридан-тўғри танишга асосланган, яъни инсон кузатуви моделлаштирилган. Пассив мониторинг тизим компьютердан иборат бўлиб, ОАВ кузатиш орқали қабул қилинган сигналнинг баъзада мавжудлиги текширилган. Агар таққосланиш

натижаси ижобий бўлса, ОАВ дастури (қўшиқ, филм, реклама ва ҳак.) идентификацияланган (ҳақиқий деб топилган). Ушбу усул текшириш тўғридан-тўғри амалга оширилади. Ушбу усулда керакли ОАВ контенини таниб олишда ҳеч қандай унга боғлиқ маълумот қўшиш (watermarking) талаб этилмайди. Бошқа сўз билан айтилганда, ОАВ контенти ҳеч қандай ўзгаришга учрамайди. Бу эса ўз навбатида ортиқча сарф-харажатларни олдини олади.

Шунга қарамасдан пассив мониторинг усулида бир нечта потенциал муаммолар мавжуд. Биринчидан, қабул қилинган сигнални базадаги сигнал билан таққослаш осон иш эмас. Амалиётда ҳар бир видео лавҳалар бир неча ўнлаб фреймларга бўлинади. Ҳар бир фрейм эса базадаги мавжудлари билан солиштирилади. Ҳар бир фрейм миллионлаб битлардан ташкил топганлигини ҳисобга олинса, бу иш катта ресурс ва вақт талаб этади. Шунинг учун дастлаб қабул қилинган сигнал, барча ўз хусусиятларини сақлаб қолган ҳолда кичик ҳажмдаги сигнатурага (масалан, хэш функцияларга асосланган) айлантирилади ва бу сигнатура базадаги мавжад сигнатуралар билан солиштирилади. Ушбу усул олдингисига қараганда бир қадар фойдалироқ саналсада, узатишда сигналларни сўниб келишини ҳисобга олинса, ҳисобланадиган сигнатуралар базадаги мавжуд сигнатуралар билан мос келиши камаяди. Шулар ҳисобга олган ҳолда, шуни айтиш мумкинки 100 % ишночли саналган пассив мониторингни амалга ошириш имконияти йўқ. Ушбу муаммлар натижасида эса *актив мониторингни* яратиш устида изланишлар олиб борила бошланди.

*Актив мониторинг*ни ОАВ контенти орқали келадиган маълум ахборот асосида амалга оширишга асосланган бўлиб, унда тўлиқ компьютер таниб олиш усулига асосланган (инсон иштирокисиз). Ушбу усул техник томондан пассив мониторинга қараганда содда бўлиб, таништирувчи маълумотни декодлаш (аниқлаш) орқали амалга оширилади. Бунда ортиқча маълумотлар базаси талаб этилмайди.

Актив мониторингни амалга оширишда қўлланиладиган усуллардан бири бу – таништирувчи маълумотни ОАВ сигналининг ажратилган соҳасида қўйишдир. Масалан, аналог телевидения ОАВ видео сигналларнинг вертикал соҳа интервалида (vertical blanking interval, VBI) рақамли маълумотларни кодлашни имконини беради. Бу маълумотлар видео сигналлар фреймлари орасида юборилади.

Аммо, VBI да қўшилган маълумот бир қанча муаммларни келтириб чиқара бошлади. Масалан, АҚШда фреймлар орасида қўйилган маълумотни бошқарувчи бўйича муаммолар келиб чиққан. Шундан сўнг, ҳар бир телекўрсатувлар учун алоҳида идентификация рақамлари берилган. Ушбу

усул аналог телевидениялар кенг фойдаланилсада, рақамли телевидениялар вужудга келиши (аналог-рақамли ва рақамли-аналог ўзгартирилишларни амалга оширилиши) натижасида бу усул самара бермай қолди.

Watermarking актив мониторингда кенг фойдаланилиб, унинг афзаллиги watermarkingни контент ичида жойлашганлигидир. Ушбу усулнинг камчилиги эса VBI га қараганда контент ичида watermarkingни жойлаштириш қийин вазифадир. Бундан ташқари, watermarkingни контент ичида жойлашганлиги видео сифатини ҳам бир қадар пасайтиради. Шунга қарамасдан ҳозирда кўплаб телевидениялар watermarkingдан актив мониторингни амалга оширишда фойдаланмоқда (Teletrax ташкилоти Philips томонидан ишлаб чиқилган видео watermarking технологиясидан фойдаланади).

1.2. Эгалик идентификацияси, эгалик тасдиғи, келишувларни аниқлаш

Эгалик идентификацияси. Одатда инсон кўзига кўринувчи контентларга экалик ҳуқуқини билдирувчи белгилар қўйилади. Бу белгилар “copyright” атамаси билан бошланади ёки унинг ўрнига © белгисидан фойдаланилади. Масалан, “Copyright *маълумот эгаси*”, “© *маълумот эгаси*”, ёки “Corp. *маълумот эгаси*” кўринишларида бўлиши мумкин (*Изоҳ:* © ўрнида (C) дан фойдаланиш бир хил қонуний аҳамият касб этмайди). Овоз маълуомотлар учун эса ℗ белгисидан фойдаланилади. Бу белги овоз маълумотлари ёзилган тасмалар устида қўйилади.

Текст кўринишидаги эгалик идентификацияси белгилари бир талай чекланишларга эга. Масалан, китоб муқовасида қўйилган эгалик белгисига тегмасдан ҳам, китоб саҳифаларини нусхалаш мумкин ёки қуйи бутун дунёда машҳур саналган “Lena” расмини олиш мумкин. Ушбу расм 1972 йилда *Playboy* ташкилоти томонидан олинган ва ундаги расмда ушбу ташкилотнинг эгалик белгиси қўйилган. Аммо, кейинчалик расмдан фақат “Lena”нинг бош қисми кесиб олинган (2.1-расм).

А)

Б)

2.1-расм. Эгалик ҳуқуқини бузулиши: А) кесиб олинган расм қисми Б) экалик белгиси мавжуд расмнинг қолган қисми

Бундан муаммони олдини олишда watermarking технологиясининг “билинмаслик” ва “ажралмаслик” хусусиятлари муҳим аҳамият касб этади. Ушбу имкониятларни ўзида мужассамлаштирган “Digimarc” иловаси ҳозирда расмларда watermarking белгисини қўйишда ва уни аниқлашда фойдаланилади. Ушбу илова Adobe фирмасининг расмларга ишлов берувчи иловаси Photoshop дастурида мавжуд.

Экалик тасдиғи. Watermarking технологияси нафақат эгалик идентификациясида (эгаликни кўрсатиш учун), балки, эгаликни тасдиқлаш учун ҳам фойдаланилади. Текст кўринишидаги эгалик белгилари эса ушбу вазифани бажара олмайди.

Бунинг бир йўли ҳар бир расмни қонуний томондан ҳимоялаш бўлиб, унга кўра расмларга махсус ташкилотлар томонидан эгалик ҳуқуқи берилади. Ушбу усул ишончли бўлиши билан бирга, нархи юқоридир.

Ушбу муаммони ҳал ечишда Digimarc иловаси ёрдам бермайди. Ушбу илова барча учун очиқ бўлиб, унга қўйилган watermarking белгисини ихтиёрий шахс билиши ва ўзгартириши мумкин.

Бу ҳолда эгаликни тасдиқлаш зарур бўлиб, бунда фақатгина бир томонга маълум бўлган детекторлардан фойдаланиш мумкин.

Ушбу муаммони ҳал этишда бошқа усул қўлланилиб, унга кўра бир расмнинг кимга тегишли эканлиги бошқа бир расм орқали тасдиқланади. Бошқа сўз билан айтганда, яратилган расмдан негатив расм олинади ва у чоп этилади. Негатив расм қалбакилаштирилган тақдирда ҳам ҳақиқий расм орқали уни тасдиқлаш имконияти мавжуд бўлади. Ушбу усул билан кейинги бўлимларда танишиб чиқилади.

Келишувларни аниқлаш. Кўплаб иловаларда watermarking белгиси келишувларни аниқлаш учун фойдаланилади. Масалан, ишлаб чиқарувчи ёки маълумот эгаси чоп этилган ҳар бир нусхага турли такрорланмас watermarking белгиларини қўяди. Бу орқали эса ноқонуний тарқалган нусхаларни ким томонидан тарқатилганилигини аниқлаш имконияти яратилади (2.2-расм).

Watermarking Applications and Their Properties

Ingemar J. Cox, Matt L. Miller and Jeffrey A. Bloom
NEC Research Institute
4 Independence Way
Princeton, NJ 08540
ingemar,mlm,bloom@research.nj.nec.com

Abstract

We describe a number of applications of digital watermarking and then examine the common properties of robustness, tamper-resistance, fidelity, computational cost and false positive rate. We observe that these properties vary greatly depending on the application. Consequently, we conclude that evaluation of a watermarking algorithm is difficult without first indicating the context in which it is to be applied.

1. Introduction

Watermarking methods are often evaluated based on the common properties of robustness, tamper resistance, and fidelity. However, examination of these properties without careful consideration of the application can often be misleading. A watermark designed to serve security needs of the CIA must meet different requirements than one intended for annotating home video. Thus, it is inappropriate to evaluate these two watermarks according to the same standards.

In this paper, we examine how the requirements for watermarking can vary with application. Section 2 briefly describes eight existing and proposed applications of watermarks. This is followed, in Section 3, with a discussion of several properties of watermarking systems, and how their definition and importance depend on the application.

2 Applications

2.1 Broadcast monitoring

In 1997, a scandal broke out in Japan regarding television advertising. At least two stations had been routinely overbooking airtime. Advertisers were paying for thousands of commercials that were never aired [15]. The practice had remained largely undetected for over twenty years, in part because there were no systems in place to monitor the actual broadcast of advertisements.

There are several types of organizations and individuals interested in broadcast monitoring. Advertisers, of course, want to ensure that they receive the airtime purchased from broadcasting firms. Musicians and actors want to ensure that they receive accurate royalty payments for broadcasts of their performances.[1] And copyright owners want to ensure that their property is not illegally rebroadcast by pirate stations.

We can use watermarks for broadcast monitoring by putting a unique watermark in each video or sound clip prior to broadcast. Automated monitoring stations can then receive broadcasts and look for these watermarks, identifying when and where each clip appears. Commercial systems have been deployed for a number of years and the basic concepts have a long history [14, 3, 18, 10, 4].[2]

2.2 Owner identification

Although a copyright notice is no longer necessary to guarantee copyrights, it is still recommended. The form of the copyright notice is usually Ó© 1998, owner.Ó It is visible on books and photographs. Copyright notices can usually be found preceding the content of videotapes and on the packaging of prerecorded video and music products. One disadvantage of such ÓhardÓ copyright notices is that they can often be removed from the protected material. Packaging can be lost, video programs can be temporally cropped, and images can be spatially cropped. A digital watermark can be used to provide complementary copyright marking functionality because it becomes an integral part of the content, i.e. the copyright information is embedded in the music to implement the ÓhardÓ notice printedon the packaging.

[1] A recent spot-check by the Screen Actors Guild found an average of $1000 in underpaid royalties per hour of US television programming [2].

[2] The earliest reference we have found [16] is assigned to the Muzak Corporation, famous for providing Ódrivin' music.Ó and may be the source of the many rumors that Muzak contained subliminal messages.

2.2-расм. Ягона идентификация рақамига эга чоп этилган текст маълумот

Мисол сифатида DiVX Corporation томонидан тақдим этилган “pay-per-view” моделидаги видео плейрларни олиш мумкин. Ушбу плейрларда кўплаб хавфсизлик усуллари қўлланилинган бўлиб, улардан бири бу – келишувни аниқлаш имкониятидир. Бунга кўра ушбу қурилма орқали кўрилган ҳар видеога ягона watermark белгиси қўйилган. Натижада, ушбу видеоларни ноқонуний кўчиришни амалга оширган шахслар аниқланган.

1.3. Контент аутентификацияси, кўчиришни назоратлаш

Контент аутентификацияси. Йилдан-йилга ўзгартирилган расм ва ҳақиқий расм орасидаги фарқни аниқлаш имконияти камайиб бормоқда. Масалан, 3-расмда келтирилган расмлар орасидаги фарқни аниқлаш шуда ҳам қийин. Бу муаммо жуда ҳам муҳим жиддий саналиб, аудио ва видео кўринишидаги маълумотларда ҳам учрайди.

2.3-расм. Ўнгда ўзгартирилган ва чапда ҳақиқий расм

Ушбу муаммони ҳал этишда криптографияда, маълум усуллар асосида хабарларни аутентификациялаш амалга оширилади. Унга асосан, бутун контент ҳақидаги маълумотни ўзида мужассамлаштирган маълумотни “рақамли имзо” деб аталиб, бу имзо ҳар бир контент учун ягона саналади. Имзони қалбакилаштириш имконияти эса мавжуд бўлмайди.

Ушбу муаммони watermarking орқали ҳал этиш имконияти мавжуд бўлиб, бунга кўра, ҳар бир контенга тегишли бўлган рақамли имзо контент узра ёйилади. Буни амалга оширишда баъзи муаллифлар томонидан қуйидаги усул таклиф этилади: расмдаги юқори даражали пикселлар асосида рақамли имзо шакллантирилиб, у паст даражали пикселлар орқасига яширинилади. Бундай ҳолда расмдаги ўзгаришлар натижасида рақамли имзо қиймати ҳам ўзгаради.

Кўчиришни назоратлаш. Кўплаб watermarking иловаларидан бузғунчи ўз ғараз ниятини амалга оширгандан сўнг уни фош этишда фойдаланилади. Баъзида эса ушбу бузғунчи вазиятлардан ҳимояланиш, уни олдини олиш талаб этилади. Бундай иловаларга нусхалашдан ҳимояловчи дастурларни олиш мумкин.

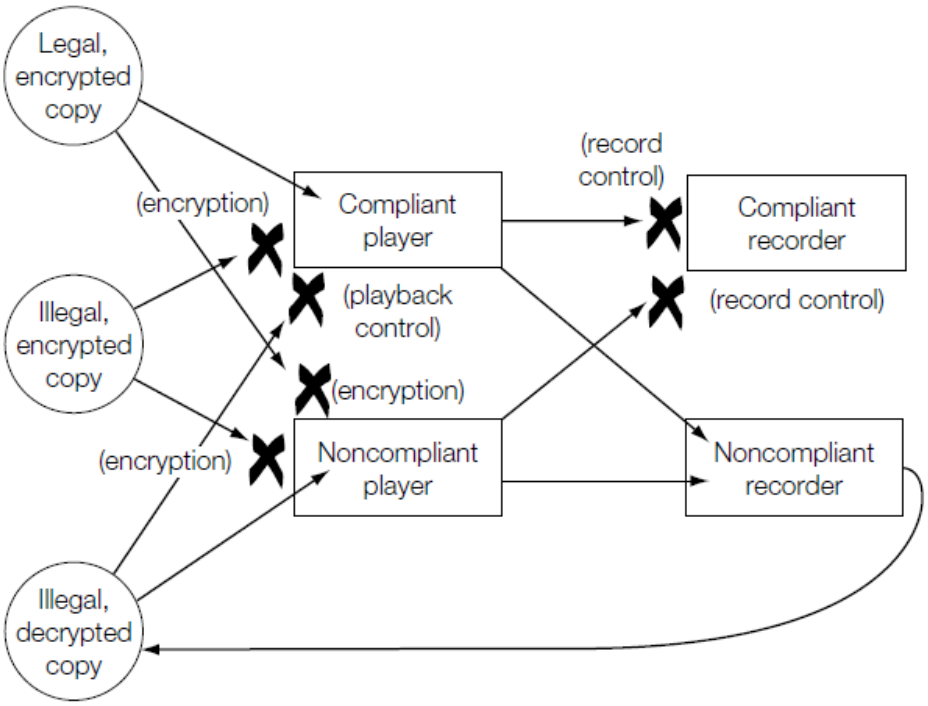
Рухсат этилмаган нусхалашдан ҳимояловчи, биринчи ва ишончли усул бу – шифрлашдир. Бундан шифрланган маълумотдан фақат махфий калит маълум бўлган шахсларгина фойдаланиши мумкин. Бундай ҳолда бузғунчи калитни билмасдан шифрланган матнни очишга ҳаракат қилиши ёки калитни ўзини топишга уриниши имконияти мавжуд бўлиб, иккаласи ҳам қийин вазифадир.

Бузғунчи юқоридаги икки усулдан фойдаланиш ўрнига, ўзи учун ҳаққоний калит олиб, шифрланган маълумотни дешифрлайди ва очиқ маълумотга эга бўлади. Бу очиқ маълумотни эса исталганча кўпайтириш имконияти мавжуд.

Watermarking белгисини бутун контент бўйлаб тарқалганлиги ҳисобга

олинса, у асосида ҳимояланиш усули мавжуд. Агар ҳар бир ёзиш қурилмалари watermarkingни аниқлаш имкониятига эга бўлганда, бу амалга оширишда муаммо бўлмас эди. Аммо бу катта муаммо саналиб, ҳар би қурилмани watermarkingни аниқлаш имкониятига эга бўлиши, истемолчилар томонидан мақулланмайди. Сабаби, истемолчиларга ўз қурилмаларида баъзи маълумотлар (watermarking белгисига эга бўлмаган) намойиш этилиши имконияти мавжуд эмаслиги ёқмаса, баъзилар эса ноқонуний тарзда нусхалашдан манфаатдор бўлади.

Шуни ҳисобга олган ҳолда, барча тасма ўқувчи қурилмаларни икки, watermarkingни танувчи, тасма ўқувчи (нусхалаш қобилятига ҳам эга) ва watermarkingни таниш қобилятига эга бўлмаган (нусхалаш қобилятига ҳам эга) турга ажратилса, улар умумий ҳолда қуйидагича тасвирланади:



2.4-расм. Шифрлаш ва Watermarkingдан фойдаланган ҳолда нусхалашдан ҳимоялаш усули

Ҳозирда (HD) DVD плейрлар ва рекордерларда watermarking технологиясидан фойдаланилган бўлиб, улар нусхалашдан ҳимоялашда фойдаланилади. Бунда овозларни ҳимоялаш учун Verance ва видеони кўчиришдан ҳимоялашда VEIL томонидан ишлаб чиқилган watermarking технологиясидан фойдаланилган. Ушбу технологиялар билан кейинги бўлимларда батафсил танишиб чиқилади.

2.4. Қурилмаларни назоратлаш, стегонаграфия иловалари

Қурилмаларни назоратлаш. Watermarking технологиясидан нафақат кўчиришдан ҳимоялашда фойдаланилади, балки қурилмаларни бошқаришда

ҳам кенг фойдаланилади. Бунга асосан, маълум вазифани бажарувчи қурилма бирор бир контентда мавжуд watermarkingни сезиши натижасида ишга тушади ёки қандайдир вазифани бажаради. Мисол сифатида, Digimarc ташкилоти томонидан мобил телефонлар учун ишлаб чиқилган тизимни олиш мумкин. Бунга кўра, мобил телефон қурилмаси фотокамераси орқали реклама газеталари, билетлар ёки бошқа қоғозлар устидаги ягона watermarking белгисини таниб олади ва фойдаланувчи у билан боғлиқ веб саҳифага кириши таъминланади.

Стегонаграфия иловалари. Стеганографик алгоритмлардан фойдаланган ҳолда махфий алоқани ташкил этиш асосида бир нечта мақсад яширинган бўлиши мумкин. Умумий ҳолда маълумот алмашадиган томонлар ўз алоқаларини бошқалардан сир тутишда фойдаланишади. Бундан мақсад, сиёсий, терроризм ёки бошқа сабаблар бўлиши мумкин. Ушбу соҳада кўплаб, иловалар ишлаб чиқилган бўлиб, уларнинг баъзилари номалум саналади ва турли ташкилотлар томонидан фойдаланилади.

Назорат саволлари

1. Watermarking технологиялари ва стегонографиянинг асосий хусусиятлари.
2. Watermarking технологиялари қандай иловаларда фойдаланилади.
3. Стегонаграфия қайси мақсадларда фойдаланилади.

Фойдаланилган адабиётлар

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, (2008). Digital Watermarking and Steganography, the Morgan Kaufmann Series in Multimedia Information and Systems, 2nd Ed.
2. Peter Wayner, (2008). Disappearing Cryptography, Second Edition - Information Hiding: Steganography and Watermarking, Morgan Kaufmann.
3. Bruce Schneier, (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C, second Edition, John Wiley & Sons.

3-маъруза

Watermarking моделлари

Режа:

1. Алоқа тармоқлари ташкил этувчилари.
2. Маълумот узатиш каналлари синфлари, хавфсиз маълумот узатиш.
3. Алоқа тармоқларига асосланган watermarking моделлари.

Таянч иборалар: Алоқа тармоғи, маълумотларни узатиш каналлари, хавфсиз маълумот узатиш, watermaking модели

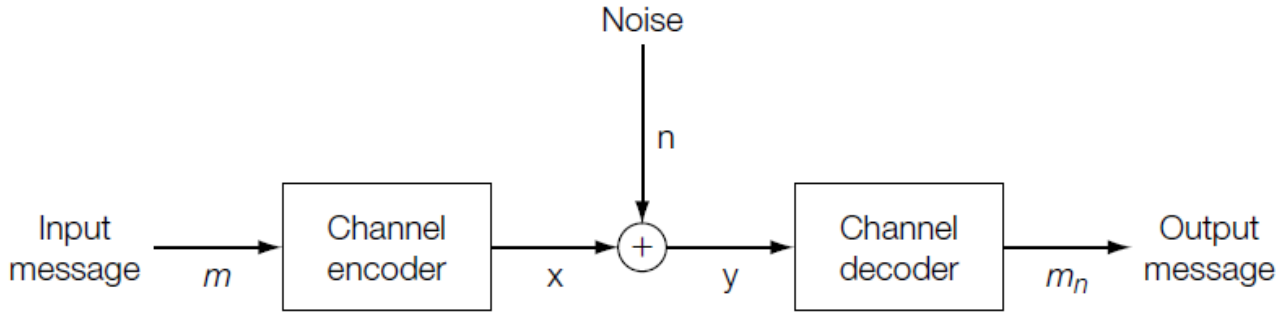
1.1. Алоқа тармоқлари ташкил этувчилари

Бундан олдинги икки маърузада рақамли watermarking ва стеганография алгоритмларининг техник бўлмаган хусусиятларига тўхталиб ўтилган эди. Бундан кейинги маърузаларда watermarking ва стеганографиянинг техник томондан хусусиятларини кўриб чиқилади. Бу маъруза фойдаланилган техник терминларнинг ва катталикларнинг тавсифи қуйида келтирилган:

Скаляр: скаляр ўзгарувчилар курсив шаклида катта ва кичик ҳарфларда ифодаланиши мумкин, масалан, N, i, x ва бошқалар. n скаляр катталикни модули $|n|$ шаклида белгиланади.

Watermarking алоқа тармоғи ва оддий алоқа тармоғи бир-бирига ўхшаш ва фарқли томони мавжуд бўлиб, қуйида улар билан батафсил танишиб чиқилади.

Одатий алоқа тармоғи. 3.1-расмда одатий алоқа тармоғи тузилиши келтирилган бўлиб, кирувчи хабар m кодер орқали кодланади ва кодланган x маълумот тармоқ орқали узатилади. Узатилиш давомида унга ташқи n шовқин маълумот қўшилади ва қабул қилувчига $y=x+n$ тарзида етиб келади. Қабул қилувчи эса декодер қурилмаси орқали декодланади ва натижавий m_n маълумот олинади.



3.1-расм. Одатий алоқа тармоғи тузулиши

Амалда рақамли сигналларда, кодерлар икки ташкил этувчи қурилмалардан, *малумотни кодлаш* ва *модулятор* қурилмаларидан иборат бўлади. Маълумотларни кодлаш қурилмаси кирувчи маълумотни келишилган стандарт (Unicode, ASCII) асосида кодлайди. Модулятор қурилмаси эса рақамли маълумотни аналог сигналга айлантиришга фойдаланилади.

Аналог шаклидаги маълумотга узатилиш давомида турли тасирлар натижасида шовқин маълумотлар қўшилади. Бу эса декодлаш қурилмасидан шовқин аралашган маълумотдан ҳақиқий маълумотни ажратиш имкониятини талаб этади.

1.2. Алоқа каналлари классификацияси, хавфсиз маълумот узатиш

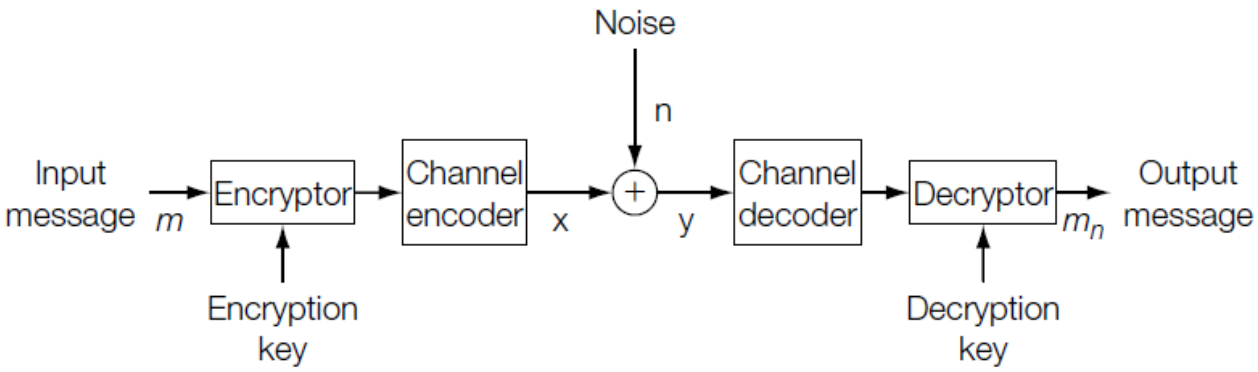
Юқоридаги 3.1-расмда келтирилганидек, шовқин маълумотлар функцияси алоқа давомида ўзгармасдир. Одатда алоқа канали *шартли тарқалиш эҳтимоллиги* қиймати, $P_{x|y}$ (у), яъни узатилган *х* сигналдан *у* сигнални олиниш эҳтимоллиги билан белгиланади.

Шовқин функцияси турига кўра алоқа каналлари турлича фарқланади. 3.1-расмда келтирилган алоқа тармоғида, *аддитив шовқин* канали тасвирланган бўлиб, унга кўра маълумотга шовқин маълумот қўшилиши натижасида сигнал ўзгаради, яъни, $y=x+n$.

Бундан ташқари *ноаддитив шовқин* каналлари мавжуд бўлиб, кенг тарқалган бундай каналга *сўниш каналини* олиш мумкин. Бунга асосан сигнал кучи вақт давомида турлича бўлади ва $y=v[t]x$, шаклида белгиланади. Бу ерда, $0 \le v[t] \le 1$. Бу каналлар бундан ташқари аддитив каналларни ҳам ўз ичига олиши мумкин, $y=v[t]x+n$.

Хавфсиз алоқа канали. Одатда алоқа каналларида маълумот узатиш давомида уларни хавфсизлигини таъминлаш муаммоси туғилади. Хавфсизликни таъминлаш деганда, маълумотни пассив ва актив таҳдидлардан ҳимоялаш тушунилади.

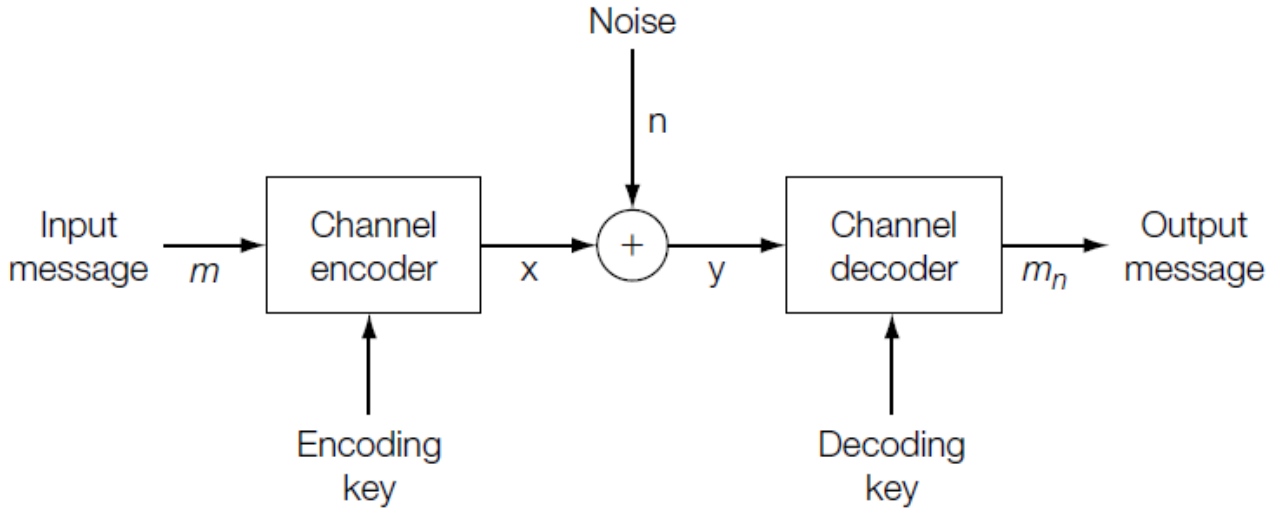
Криптографик ҳимоялаш усуллари орқали ҳар иккала турдаги таҳдидларни бартараф этиш мумкин. Бунга асосан, *очиқ* маълумот *калит* орқали шифрланиб, *шифрматн*га айлатирилади. Шифрматн эса алоқа канали орқали узатилади. Қабул қилишда шифрматн калит асосида дешифрланиб, очиқ матн олинади.



3.2-расм. Шифрлашга асосланган алоқа канали

Шунга қарамасдан, криптографик ҳимоя маълумотни узатилишини яшириш имкониятини бермайди. Бундан ташқари ушбу каналда бузғунчи томонидан шифрланган матнни ўчириб ташлаш имконияти мавжуд бўлиб, кўп ҳолларда бу катта муаммоларни келтириб чиқаради.

Бу турдаги муаммоларни ҳал этишда *кенг полосали псевдотасодифий алоқа тизимлари (spread spectrum communication)* тизимлари ривожланиши катта таъсир ўтказди. Бу тизимга кўра, махфий *код* асосида модуляция жараёни амалга оширилиб, узутилаётган сигнал кенг поласалар бўйлаб тарқалади (3.3-расм).



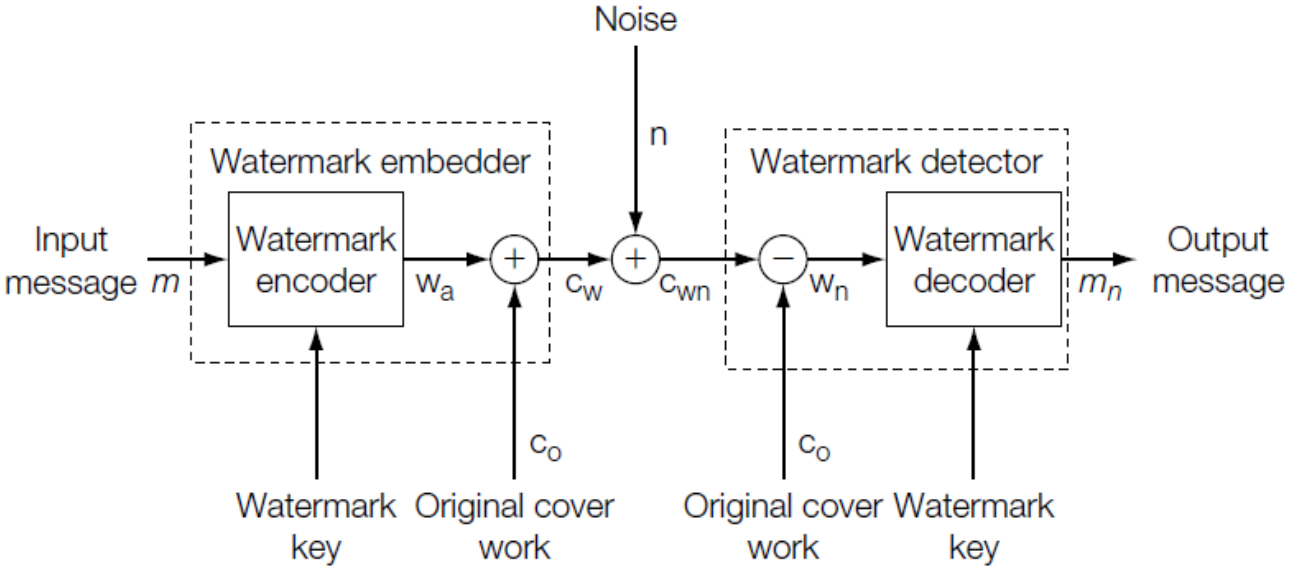
3.3-расм. Кенг полосали псевдотасодифий алоқа тизимлари

Баъзида криптографик ҳимоя воситаси ва кенг полосали псевдотасодифий алоқа тизимлари бираликда фойдаланилади. Криптографик ҳимоялаш усули маълумотни махфийлигига жавоб берса, кенг полосали псевдотасодифий алоқа тизимлари эса шифрланган маълумотни яшириш учун фойдаланилади.

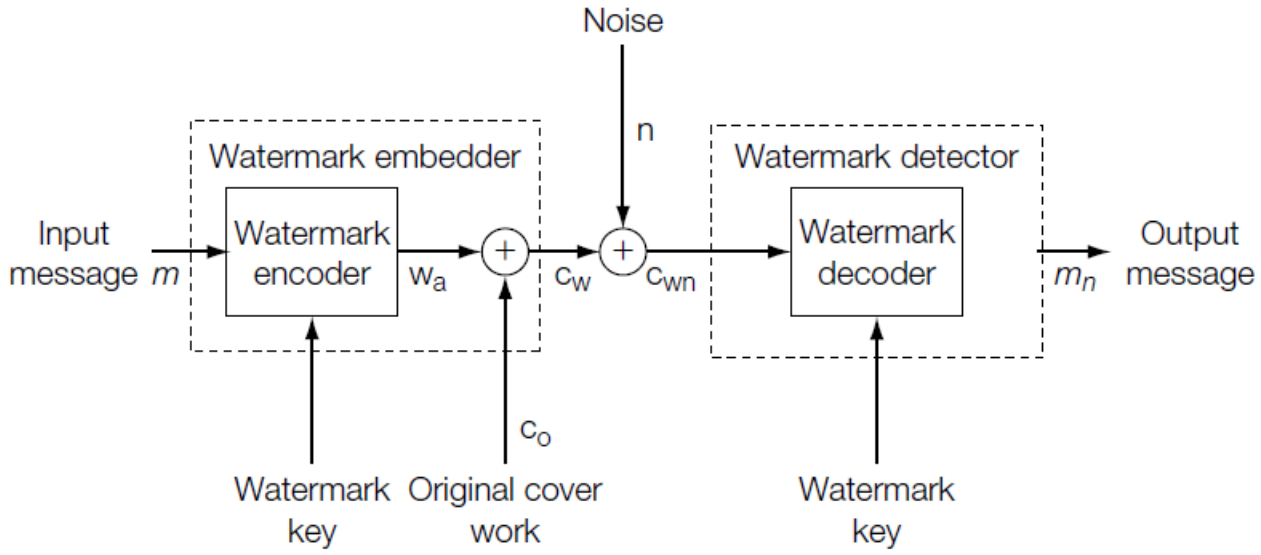
1.3. Алоқа каналларига асосланган watermarking моделлари

Watermarking тизими ҳам алоқа тури ҳисобланиб, бошқа сўз билан айтганда одатий алоқа каналига watermarking тизими киритилади. Watermarking тизимларини одатий тизим ичида киритишда контентнинг қандай тарзда бирлаштирилганига кўра алоқа каналларига асосланган watermarking моделлари, қуйидаги уч турга ажратилади:

Асосий модел. Бу моделда 3.3-расмда келтирилган тизимда watermarking тизими киритилади. Бунда икки ҳолат, информатив детектор ва кўркўрона детектор киритилган ҳол қуйидаги 3.4,3.5-расмларда келтирилган.



3.4-расм. Информатив детектор

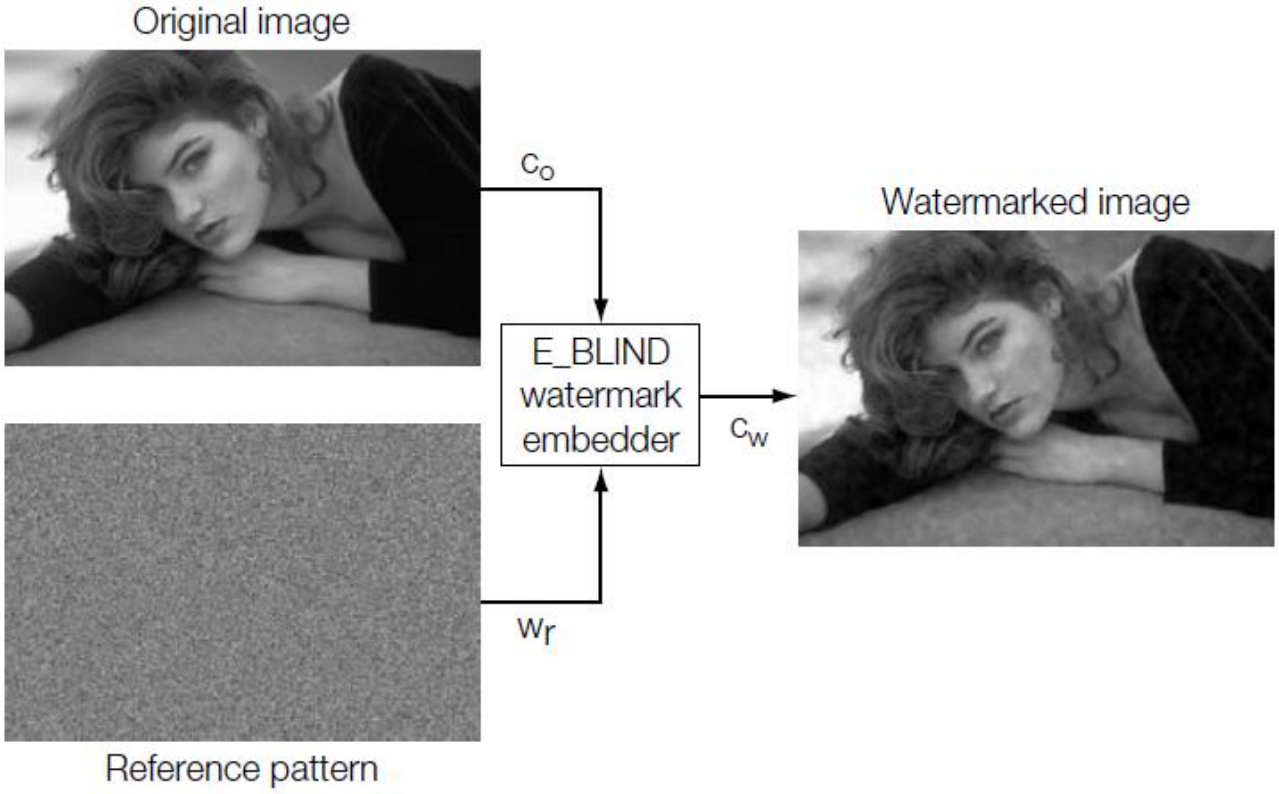


3.5-расм. Кўркўрона детектор

Ҳар иккала ҳолатда ҳам, watermarkingни қўйиш (эмбеддинг) жараёни

икки қадамдан иборат бўлади. Дастлаб, маълумот (Input message) watermarking шаблони, $\mathbf{w_a}$ ичига киритилади. $\mathbf{w_a}$ маълумотни яширувчи контент (cover Work, $\mathbf{c_0}$) билан бир хил ўлчам ва турга эга. Масалан, watermarking маълумот расм бўлса, унда маълумот яширувчи контент ҳам расм бўлиши талаб этилади. Watermarkingни қўйишда шароитга кўра *калитдан (watermark key)*дан фойдаланиш мумкин.

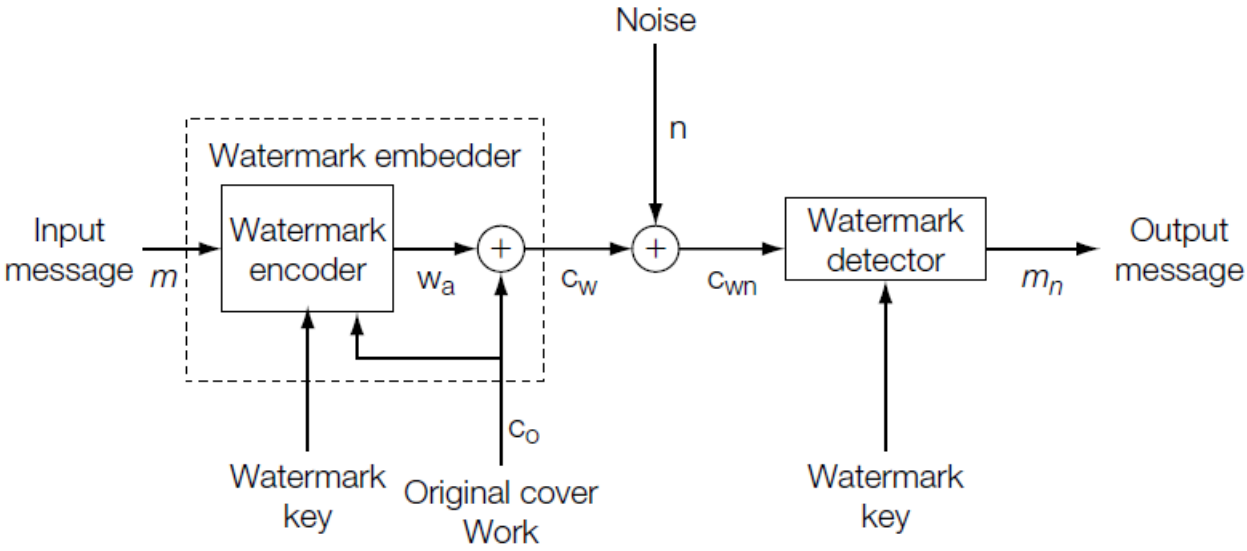
Шундан сўнг, $\mathbf{w_a}$ ва $\mathbf{c_0}$ маълумотлан қўшилади ва watermarking белгисига эга контент, $\mathbf{c_w}$ ҳосил қилинади. Кўркўрона детекторлашда тасодифий ҳолда watermarking белги аниқланади. Информатив детекторда эса детекторлаш икки босқичда амалга оширилади. Биринчи бўлиб, watermarking қўйилмаган контент ($\mathbf{w_n}$) қабул қилинган маълумотдан ($\mathbf{c_{wn}}$) ажратилиб олинади. Шундан сўнг, калит асосида декодланади.



3.6-расм. Декодлаш жараёни

Узаткичдаги қўшимча маълумотлар ёрдамида алоқа тизими кўринишидаги watermarking модели. 3.5-расмда келтирилган тизим кўплаб фойдаланилаётган watermarking қўйиш тизимларини қўллаб – қувватламайди. Сабаби, қўйилган watermark маълумотни яширувчи контенга боғлиқ эмас. Кўплаб амалда фойдаланилаётган watermarking алгоритмлари маълумот яширувчи контент $\mathbf{c_0}$ ва watermarking шаблони $\mathbf{w_a}$ ларни watermarkingни кодлашдан олдин қўшиш имконияти мавжуд. Қуйидаги 3.7-расмда ҳосил бўлган $\mathbf{w_a}$ маълумот $\mathbf{c_0}$ боғлиқдир. Ушбу тизим 3.5-расмда келтирилган тизим билан бир-хил бўлиб, фарқли томони watermarkingни

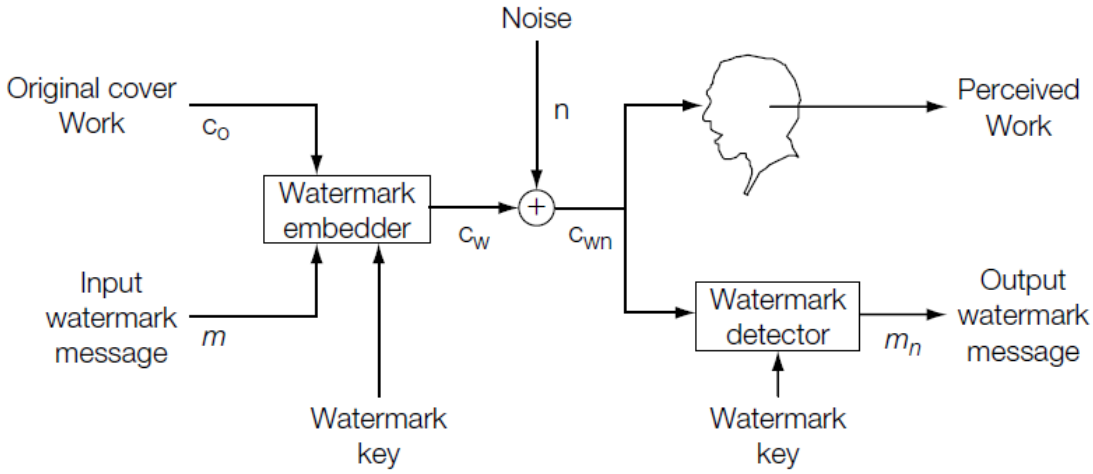
кодлашда қўшимча $\mathbf{c_0}$ контент киритилмоқда.



3.7-расм. Кодлаш жараёни

Бунда $\mathbf{c_w}$ нинг ўзгариши $\mathbf{w_a = c_w - c_0}$ натижасида юз беради. Агар алоқа каналида $\mathbf{c_0}$ ни шовқин маълумотнинг бир қисми ($\mathbf{c_0+n}$) деб ҳисобланса, янги модел ҳосил бўлади, яъни *узаткичдаги қўшимча маълумотлар ёрдамида алоқа тизими кўринишидаги watermarking модели*. Бу ва юиринчи моделга кўра, маълумот яширувчи контент алоқа тармоғининг бир қисми сифатида ҳисобланади.

Кўп тармоқли (мултипликатор) тармоқ шаклидаги watermarking модели. Бу моделга асосан маълумотни яширувчи контен тармоқнинг бир қисми сифатида фойдаланилмай, балки, $\mathbf{c_w}$ ҳосил қилишда керакли бўлган иккинчи сигнал сифатида олинади. Қабул қилинишда эса, $\mathbf{c_0}$ ва $\mathbf{m}$ сигналлар иккита турли қабул қилгичлардан фойдаланилади: инсон ва watermarking детектор.



3.8-расм. Кўп тармоқли (мултипликатор) тармоқ шаклидаги watermarking модели

Назорат саволлари

1. Алоқа тармоғининг ташкил этувчилари
2. Маълумотларни узатиш каналларининг классификацияси
3. Watermarking моделлари

Фойдаланилган адабиётлар

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, (2008). Digital Watermarking and Steganography, the Morgan Kaufmann Series in Multimedia Information and Systems, 2nd Ed.
2. Peter Wayner, (2008). Disappearing Cryptography, Second Edition - Information Hiding: Steganography and Watermarking, Morgan Kaufmann.
3. Bruce Schneier, (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C, second Edition, John Wiley & Sons.

4-маъруза

Асосий хабар кодлаш усуллари

Режа:

1. Тўғридан-тўғри хабарларни кодлаш.
2. Кўп белгили хабарларни кодлаш.
3. Хатоликларни тузатиш кодлари, Хэмминг коди.

Таянч иборалар: хабарларни кодлаш, кўп белгили хабарларни кодлаш, хатоликлар, хэмминг коди.

1.1. Тўғридан-тўғри хабарларни кодлаш

Watermarking тизимларида маълумот узунлиги бир бит бўлганда, уни контентга бирлаштириш муаммо саналмайди. Аммо, амалиётда кўплаб иловалар бир битдан кўп маълумотларни талаб этади. Ушбу маърузада маълумотларни watermarking белгилари сифатида ифодалаш усуллари ва хатоликларни тузатиш кодлари ҳақида тўхталиб ўтилади.

Тўғридан-тўғри хабарларни кодлаш усули бир-бирига боғлиқ бўлмаган хабар белгилари кетма-кетлигини контентларга жойлаштириш орқали амалга оширилади. Ушбу усулда асосан маълумотлар иккилик шаклида ифодаланади.

Масалан, барча қўйилиши керак бўлган хабарлар кетма-кетлиги M бўлиб, ушбу кетма-кетликлар сони |M| га тенг. Ушбу хабар кетма-кетлигидан |M| та хабар белгилари, W ҳосил қилинади.

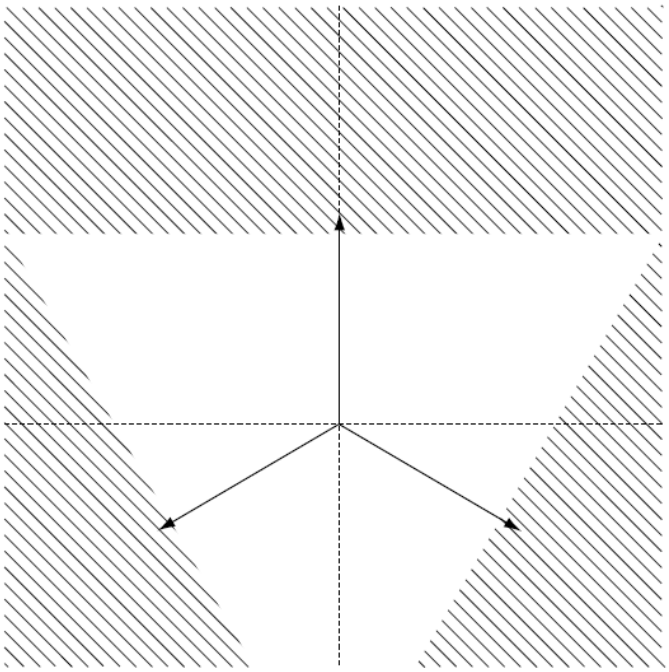
Биз хабар билан боғлиқ хабар белгиларини ифодалаш учун *W[m]* тарзида ифодалаб, бу ерда *m* хабар бўлиб, $m \in M$. Контентга *m* хабар белгисини қўйиш учун, унга *W[m]* хабарни бирлаштириш амалга оширилади. Ушбу кетма-кетлик *тўғридан-тўғри кодлаш* усули деб ҳисобланади.

Контентга қўйилган белгиларни текширишда, детекторлар |M| та хабар белгиларини ҳисоблаб чиқади. Бунда детектор энг яқин деб топилган хабар белгисини олади. Ушбу яқинлиликни ҳисоблашда одатда чегара қиймати (threshold) олинади. Ушбу қийматдан юқори бўлган барча қийматлар белги сифатида олинади.

Юқоридаги жумладан келиб чиқиб шуни айтиш мумкинки, детектор хабарлар кетма-кетлигини тўғри аниқлаши учун, контенга қўйилган хабарлар бир-биридан катта фарқ қилиши талаб этилади. Бошқа сўз билан айтганда ҳар бир *W[m]* бир бирига боғлиқ бўлмаслиги керак ёки яхши *ажратилганлик* даражасига эга бўлиши керак.

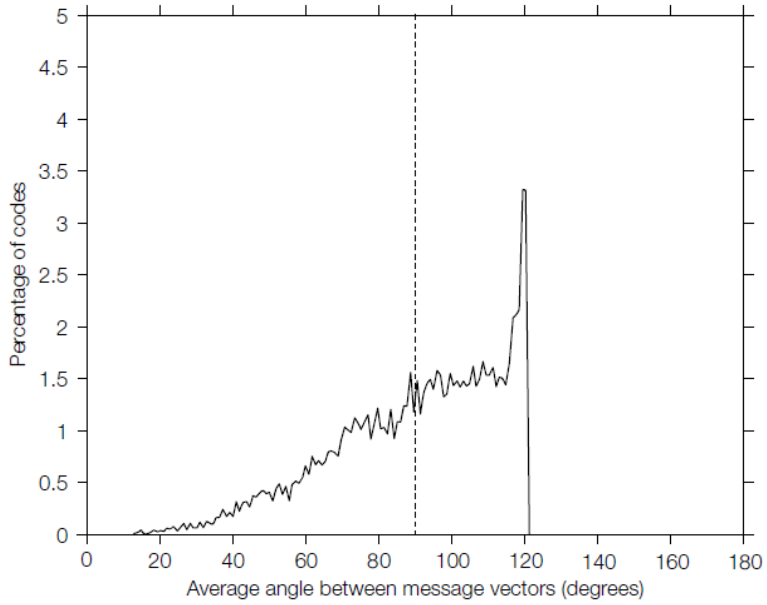
Хабарлар орасидаги фарқни аниқлашда *чизиқли ва нормал боғлиниш* функциялари кенг фойдаланалиб, агар боғлиқлик даражаси қанча кичик бўлса ажратилганлик даражаси шунча катта бўлади. Амалда эса *негатив боғланиш* функцияларидан кенг фойдаланилади.

Агар |M| лар сони учта бўлса, улар орасидаги фарқ 120 градус бўлиши талаб этилади (4.1-расм). Ушбу вазиятда хабарлар сони учта ва хабарларни ифодалаш майдони иккига тенг, яъни икки ўлчовли баҳолаш майдони (ХУ).



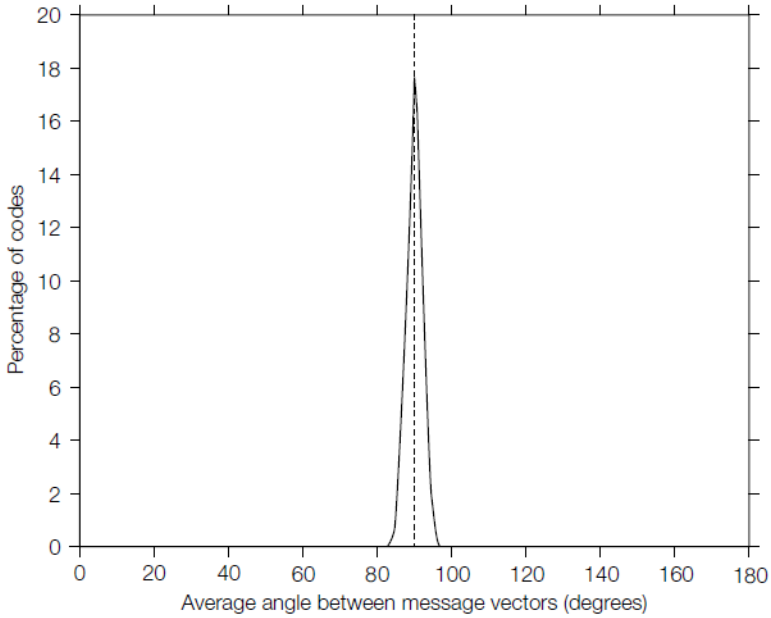
4.1-расм. Икки ўлчовли майдон

Агар хабарлар сони майдон ўлчамига қараганда жуда катта бўлган тақдирда, тасодифий кодларни ҳосил қилиш генераторларидан кенг фойдаланилади (4.2-расм). Ушбу расмда 10.000 марта учта маълумотдан иборат бўлган хабар (|M|=3) ларни уч ўлчовли майдонда ифойдалаганда улар орасидаги ўртача масофа келтирилган.



4.2-расм. Хабарлар сони майдон ўлчамига қараганда жуда катта бўлган ҳол

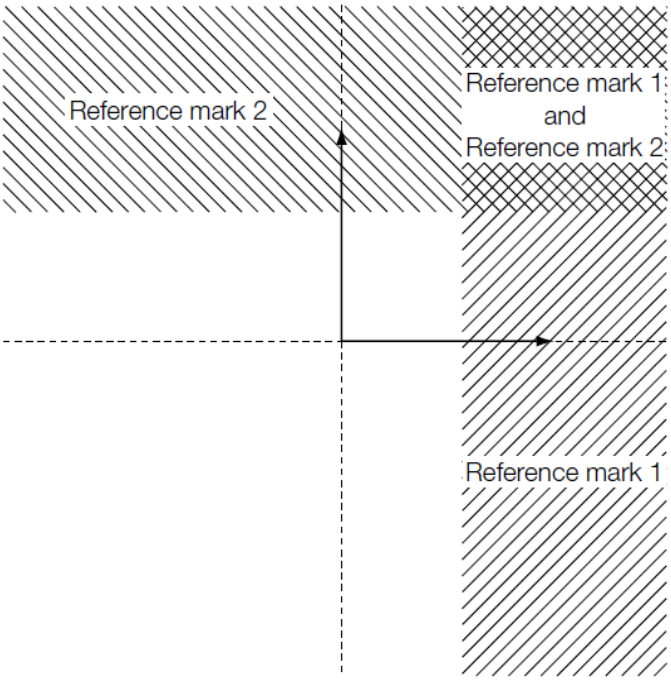
Агар хабарлар сони баҳолаш майдони ўлчамига қараганда кичик бўлса, тасодифий кодларни ҳосил қилиш генераторлари орқали ҳосил қилинган маълумотлар бир-бирига нисбатан тўғри бурчакни (ортогонал) ҳосил қилади (4.3-расм). Ушбу расмда генератор орқали ҳосил қилинган учта хабардан иборат маълумотлар 256 ўлчовли майдонда тарқалганда, улар орасидаги бурчакни ифодаси келтирилган.



4.3-расм. Хабарлар сони баҳолаш майдони ўлчамига қараганда кичик бўлган ҳол

Ортогонал хабарларни фойдали хусусияти шундан иборатки, бир контентда биттадан кўп бўлган хабарларни жойлаштириш имконияти

мавжуд. Бунда жойлаштирилган хабарлар бир-бирига тасир қилмайди (4.4-расм).



4.4-расм. Ортогонал хабарларни кодлаш

Юқоридаги расмда, икки ўлчовли майдонда икки ортогонал хабарни ифодалаш келтирилган бўлиб, бунда учта қисм майдон ифодаланган. Биринчиси биринчи хабар белгиси учун, иккинчиси иккинчи хабар белгиси учун ва учунчиси иккита хабар белгилари кесишган ҳолат учун.

1.2. Кўп белгили кодлаш

Тўғридан-тўғри кодлаш усули самарали бўлсада, кенгайтиришга қулай эмас. Сабаби, детектор мавжуд |M| та хабар белгиси учун ҳисоблашни амалга ошириш талаб этилади. Агар |M| катта бўлган тақдирда, ҳисоблашларни амалга ошириш мураккаблашиб кетади. Масалан, |M|=16 га тенг бўлса, умумий ҳисоблаш сони 65536 тани ташкил этади. Агар |M|=100 бўлган тақдирда буни ҳисоблашни имкони бўлмай қолади.

Ушбу муаммони ҳал этишнинг биринчи усули бу – хабарларни *A* *алфавит* белгиларидан тузулган белгилар кетма-кетлиги сифатида ифодалашдир. Кетма-кетликдаги ҳар бир белги контентга қўйилади ва алоҳида детектор орқали аниқланади.

Агар кетма-кетлик L та турли белгидан иборат бўлса, алфавит ўлчами $|A|$ га тенг бўлса, барча хабарлар сони $|A|^{L}$ га тенг бўлади. Масалан, $L=8$ ва $|A|=4$ га тенг бўлса, умумий хабарлар сони $|A|^{L}=4^{8}=65536$ тага тенг бўлади ёки 16 битлик хабардир. Ушбу ҳолатда детектор саккизта белгини аниқлаш учун умумий ҳолда 32 та комбинацияни бажаради. Бу эса тўғридан-тўғри

кодлашдаги 65536 та комбинацияга қараганда анча кичик қиймат.

Буни амалга оширишнинг содда усули ҳар бир кетма-кетлик белгиларини мустақил равишда контентга жойлаштириш саналиб, ушбу ёндошув устида ҳозиргача изланишлар олиб борилмоқда. Бунинг ўрнида, дастлаб кетма-кетликнинг барча белгилари модулятор орқали ягона хабар белгисига ўтказилади ва кейин ушбу хабар белгиси эмбеддер орқали контентга бирлаштирилади. Қуйида буни амалга оширишда фойдаланиладиган модулятор кўринишлари келтирилган.

Вақт ва майдон бўйича модуляция (Time - and Space-Division Multiplexing). Бу модуляция усулида хабар белгилари контент бўйича майдон ёки вақт узунлиги бўйлаб тақсимланади. Яъни, бир қисмда битта белги жойлаштиралади. Умумий хабар белгилари эса барча қисмларда қўйилган қисм хабар белгиларини бирлаштириш орқали олинади.

Масалан, 8 га тенг узунликдаги хабар кетма-кетлигини *L* узунликдаги аудио контентига жойлаштиришда, *L/8* тақсимотидан фойдаланилади. Яъни, контентнинг 1/8 қисмига хабарнинг битта белгиси бириктирилади. Бундан ташқари, 4 та белгидан иборат хабар кетма-кетлигини ўлчами *w*h* пикселга тенг расмда жойлаштириш учун, ҳар бир пиксел *w/2*h/2* майдонида жойлаштирилади.

Юқорида келтирилган модуляция усуллари *вақтни тақсимлашга ва майдонни тақсимлашга асосланган модуляция* деб аталади.

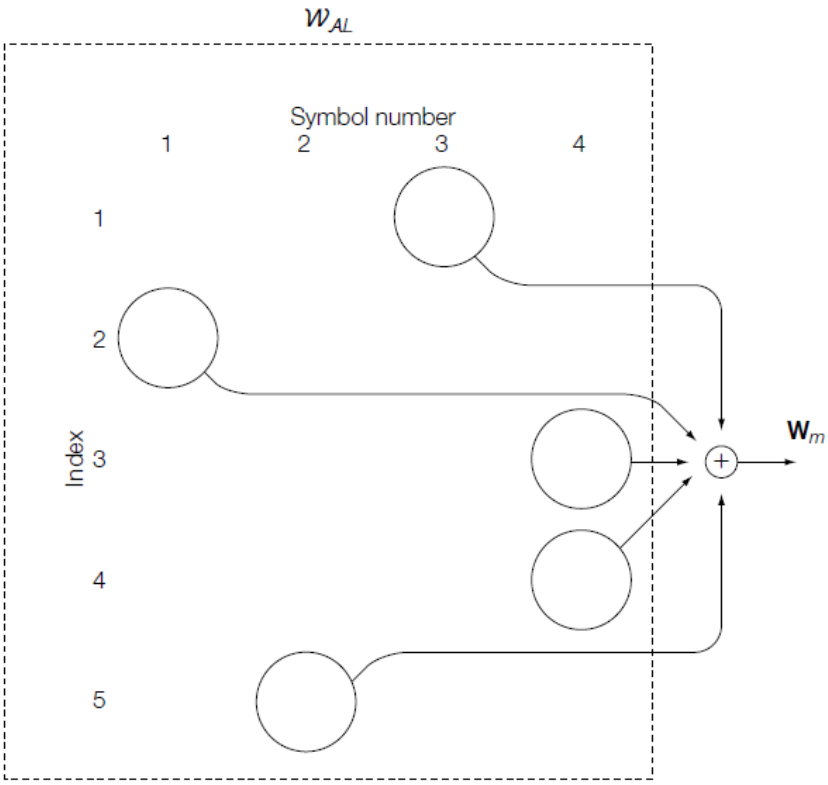
Частота бўйича модуляция (Frequency-Division Multiplexing). Модуляциянинг бу усулга асосан контент частоталар бўйича қисмларга ажратилади ва ҳар бир қисмга хабарнинг бир белгиси бириктирилади. Натижавий хабар эса турли частоталар қисмларида бириктирилган маълумотларни бирлаштириш натижасида олинади.

Кодлашга асосланган модуляция. Агар хабар *L* узунликдан иборат бўлса ва белгилар узунлиги |*A*| га тенг алфавитдан олинган бўлса, бунда умумий ҳолда *L*|A|* та вариантни, W_{AL} ҳисоблаш мумкин бўлади. Унда уни $W_{AL}[i,s]$ деб белгиланса, бунда *s* кетма-кетликдаги *i* ўринда турган белги.

4.5-расмда расм 8x8 ўлчамга эга бўлган қисмларга ажратилган ва маълумотлар ҳам 8x8 га ажратилган ҳолат келтирилган. 8x8 жадвал ва $W_{AL}[1. . . 5, 1. . . 4]$ катталиклар хабар белгилари кетма-кетлиги узунлиги *L=5* ва алфавит узунлиги |*A*|=*4* ҳолат модуляциясида фойдаланилади. Белгилар кетма-кетлиги 3,1,4,4,2 га тенг ҳолат учун кодлаш жараёни қуйидагича:

$$w_m = W_{AL}[1, 3] + W_{AL}[2, 1] + W_{AL}[3, 4] + W_{AL}[4, 4] + W_{AL}[5, 2]$$

бу ерда w_m - натижавий хабар белгиси.



4.5-расм. Кодлашга асосланган модуляция

Ушбу ифодани ҳосил қилишда қўшилувчи ҳар бир белгилар ўзаро - ортогонал бўлишига ёки камида унга яқин бўлишига этибор бериш керак. Яъни, бир позицияда жойлашган белгилар ўзаро қўшилмайди ёки белгиларни ўзаро қўшиш учун улар турли позицияларда жойлашган бўлиши талаб этилади. Масалан, $W_{AL}[1, 3]$ ва $W_{AL}[2, 1]$ белгиларни ўзаро қўшиш мумкин аммо, $W_{AL}[1, 3]$ ва $W_{AL}[1, 1]$ ўриндаги белгиларни қўшиб бўлмайди. Шунинг учун, бу шартни бажаралишида камида (a = b), $W_{AL}[i, a] \cdot W_{AL}[j, b] \approx 0$ агар $i \neq j$ бўлган шарт бажарилиши керак.

1.3. Хатоликларни тузатиш кодлари, Хэмминг коди

Амалда белгиларни контент бўйлаб тарқатиш ҳар доим ҳам самарали амалга оширилмайди. Бунинг натижасида эса белгиларни аниқлашда уларнинг айрим қисмлари аниқланмайди. Бу камчиликларни тузатишда одатда хатоликларни тузатиш кодлари (error correction codes) кенг фойдаланилади. Хатоликларни тузатиш кодларнинг моҳияти ҳар бир хабар маълумотига мос кетма-кетликдаги назорат белгиларини қўшиш орқали амалга оширилади. Қуйида юборилган ва қабул қилинган кодларнинг фарқи келтирилган.

-Юборилган: 1 1 0 0 1 0 1 0 1 1 1 0 0 0 0 1 0

Қабул қилинган: 1 1 0 1 1 0 1 0 0 0 1 0 0 0 0 1 0

Икки турдаги кодлар, хатоликларни аниқловчи ва тузатувчи кодлар

ажратилиб, хатоликларни аниқлаш кодлари фақат хабардаги кодларда хатолик мавжудлигини аниқласа, хатоликларни тузатиш кодлари эса аниқлаш билан бирга топилган хатоликларни тузатиш қобилятига ҳам эгадир.

Хатоликларни тузатиш кодларининг умумий кўриниши қуйидагича:

k – Маълумот ўлчами (битда, байтда).

m – Қўшилувчи маълумот ўлчами (битда, байтда).

n = k+m – код сўз узунлиги.

Ҳемминг масофаси деб – код сўзлар орасидаги энг кичкина масофа тушинилади. Ушбу масофани топишда икки бинар векторлар бир хил узунликда олинади ва улар XOR амалида қўшилади. Натижавий вектордаги битлар сони хэмминг масофасини, *d* ни ифодалайди.

Агар хэмминг масофаси энг кичик топилса, ушбу хатоликни тузатиш коди:

d_{min} *-1* – та х-атоликни аниқлай олади;

[(d_{min} *-1*)/2] – Хатоликни тузата олади.

Хатоликларни тузатиш кодлари одатда (n,k) шаклида белгиланади. Қуйида мисол тариқасида Хэмминг коди ифодаси берилган.

Хемминг коди оддий чизиқли блок код бўлиб, минимал код масофаси 3 га тенг, яъни бу код битта хатоликни тузатаолади. Хемминг коди бошқа кодларга ўхшаб k информацион ва (n-k) ортиқча символларга эга. Коднинг ортиқчалик қисми шундай қуриладики, декодлаш натижасида нафақат қабул қилинган комбинациядаги хатолик мавжудлигини, балки хатолик содир бўлган ўрин номерини аниқлаш мумкин бўлади. Бунга қабул қилинган комбинацияни кўп марта жуфтликка текшириш эвазига эришилади. Текширишлар сони ортиқча символлар сонига, яъни (n - k) га тенг. Ҳар бир текширишда информацион символларнинг бир қисми ва ортиқча символлардан бири қатнашади. Ҳар бир текширишдан сўнг иккили назорат символи олинади. Текшириш натижаси жуфт сонни берса назорат символига 0 қиймати, тоқ сонни берса 1 қиймати берилади. Барча текширишлар натижасида бузилган символлар ўрнининг номерини кўрсатувчи (n - k) хонали иккили сон олинади. Хатоликни тузатиш учун фақат ушбу символ қийматини тескарисига ўзгартириш кифоя.

Хемминг кодининг узунлиги n $2^k \leq \frac{2^n}{1+n}$ формула ёрдамида аниқланади. Хемминг усулига биноан текширувчи символлар қиймати ва ўринларининг номери код комбинациясининг текширувчи гуруҳларини танлаш билан бир вақтда белгиланади. Бунда қуйдагиларга асосланмоқ лозим.

Биринчи текшириш натижасида бузилган символ ўрни номерини

кўрсатувчи назорат кодининг кичик хонаси рақами олинади. Агар биринчи текшириш натижаси 1 ни берса, демак текширилган гурухнинг битта символи бузилган ҳисобланади.

Символлардан қайси бирининг бузилганлигини аниқлаш учун қуйидаги жадвалга мурожаат этамиз. Ушбу жадвалда тўрт хонали назорат сонларининг натурал қатори иккили саноқ системасида келтирилган.

4.1 – жадвал

№ k/ k	Назорат сон символларининг хоналари			
	4	3	2	1
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
10	1	0	1	0

Жадвалдан кўриниб турибдики, агар назорат сонининг кичик хонасида 1 бўлса, бузилиш код комбинациясининг тоқ ўринларида бўлади. Демак, биринчи текшириш ўз ичига тоқ номерли символларни, яъни 1, 3, 5, 7, 9, . . . ларни олади.

Агар иккинчи текшириш натижаси 1 ни берса, назорат сонининг иккинчи хонасида 1 ни оламиз. Демак иккинчи текшириш ўз ичига иккинчи хонасида 1 бўлган символларни, яъни 2, 3, 6, 7, 10 . . . ларни олади.

Худди шундай, учинчи текшириш ўз ичига учинчи хонасида 1 бўлган символларни, яъни 4, 5, 6, 7, 12 . . . ларни олади ва ҳ.

Бу каби мушохадалар қуйидаги текшириш жадвалини шакллантиришга имкон беради.

Текшириш номери	Текширилувчи ўринлар номери	Назорат символлари ўринларининг номери
1	1, 3, 5, 7, 9, 11, 13 . . .	1
2	2, 3, 6, 7, 10 . . .	2
3	4, 5, 6, 7, 12 . . .	4
4	8, 9, 10, 11, 12 . . .	8
.	. . . . .	.
.	. . . . .	.
.	. . . . .	.

Агар текширилувчи код комбинациясининг символларини a_i орқали, текширувчи амалларни S_i орқали белгиласак, қуйидагини ёзиш мумкин.

$$S_1 = a_1 \oplus a_3 \oplus a_5 \oplus a_7 \oplus a_9 \oplus \ldots$$
$$S_2 = a_2 \oplus a_3 \oplus a_6 \oplus a_7 \oplus a_{10} \oplus \ldots$$
$$S_3 = a_4 \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_{12} \oplus \ldots$$
$$S_4 = a_8 \oplus a_9 \oplus a_{10} \oplus a_{11} \oplus a_{12} \oplus \ldots$$

Назорат символларини текширилувчи гурухларнинг фақат биттасида учрайдиган номерли ўринларда жойлаштириш қулай ҳисобланади (юқоридаги жадвалга қаралсин). Жадвалга мувофиқ бу ўринлар номери 1, 2, 4, 8, . . . Демак, код комбинациясида a_1, a_2, a_4, a_8 . . . символлар текширувчи, a_3, a_5, a_6, a_7, a_9 . . . символлар информацион ҳисобланишлари лозим.

Информацион символлар қиймати олдиндан маълум бўлганлиги сабабли, текширувчи символларнинг қиймати шундай бўлиши лозимки, ҳар бир текширувчи гурухдаги бирларнинг йиғиндиси жуфт сон бўлсин.

2. 10011 иккили комбинациянинг Хемминг кодини топиш сўралсин.

Ечиш.

Информацион символлар сони k = 5. $2^k \leq \frac{2^n}{1+n}$ формулага биноан $32 \leq \frac{2^n}{1+n}$. Демак, Хемминг кодининг узунлиги n = 9. Информацион символ a_3, a_5, a_6, a_7, a_9 бўлганлиги сабабли, кўрилаётган код учун қуйидагини ёзиш мумкин.

$$a_3 = 1; \quad a_5 = 0; \quad a_6 = 0; \quad a_7 = 1; \quad a_9 = 1.$$

Текширувчи символлар қиймати йиғиндилар жуфтлигини таъминлаш шартига биноан қуйидагича аниқланади.

$$S_1 = a_1 \oplus 1 \oplus 0 \oplus 1 \oplus 1; \qquad a_1 = 1.$$
$$S_2 = a_2 \oplus 1 \oplus 0 \oplus 1; \qquad a_2 = 0.$$
$$S_3 = a_4 \oplus 0 \oplus 0 \oplus 1; \qquad a_4 = 1.$$
$$S_4 = a_8 \oplus 1; \qquad a_8 = 1.$$

Демак, оддий беш хонали код 10011 га қуйидаги тўққиз хонали Хемминг коди мос келади.

1 0 1 1 0 0 1 1 1

Фараз қилайлик, узатишда бешинчи символда хатолик рўй берди, яъни код қуйидаги кўринишни олди.

1 0 1 1 1 0 1 1 1

Текшириш қуйидагича амалга оширилади.

Биринчи текшириш:

$S_1 = 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1;$ 1.

Иккинчи текшириш:

$S_2 = 0 \oplus 1 \oplus 0 \oplus 1;$ *0.*

Учинчи текшириш:

$S_3 = 1 \oplus 0 \oplus 0 \oplus 1$ *1.*

Тўртинчи текшириш:

$S_4 = 1 \oplus 1;$ *0.*

Шундай қилиб, текшириш натижасида 0101 иккили сон олинди. Демак, хатолик бешинчи символда содир бўлганлиги исботланди.

Назорат саволлари

1. Тўғридан-тўғри кодлаш.
2. Кўп белгили кодлаш.
3. Хатоликларни тузатиш кодлари.
4. Хэмминг коди.

Фойдаланилган адабиётлар

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, (2008). Digital Watermarking and Steganography, the Morgan Kaufmann Series in Multimedia Information and Systems, 2nd Ed.
2. Peter Wayner, (2008). Disappearing Cryptography, Second Edition - Information Hiding: Steganography and Watermarking, Morgan Kaufmann.
3. Bruce Schneier, (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C, second Edition, John Wiley & Sons.

5-маъруза

Қўшимча маълумотлар асосида watermarking

Режа:

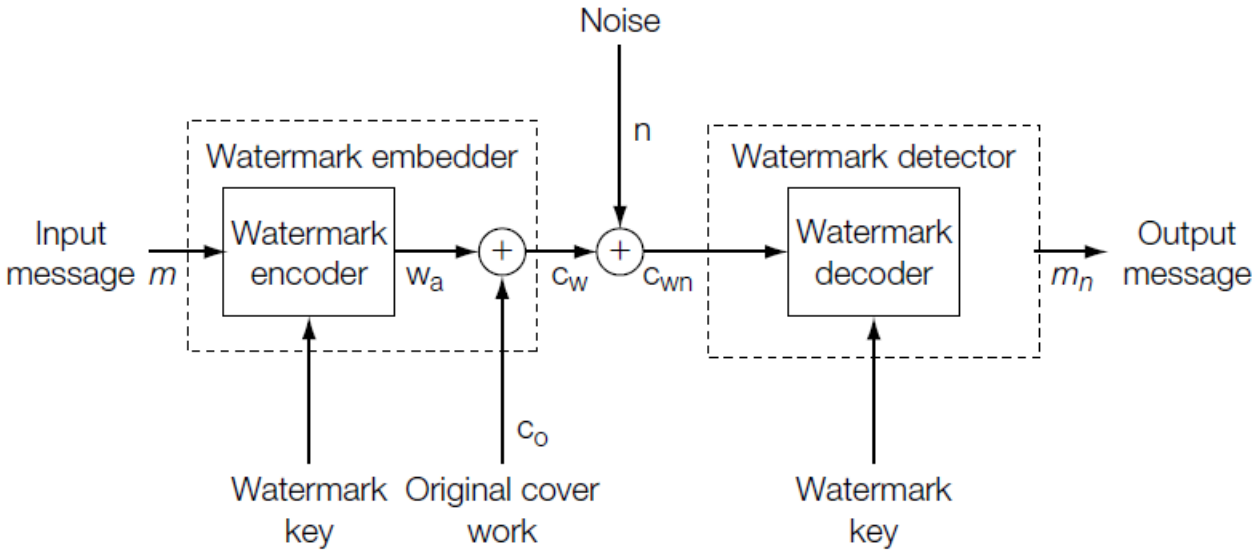
1. Информатив эмбеддинг.
2. Dirty-paper коди асосида watermarking тизими.

Таянч иборалар: Информатив эмбеддинг, кўркўрона детектор, Dirty – paper коди, шовқин, калит, контент.

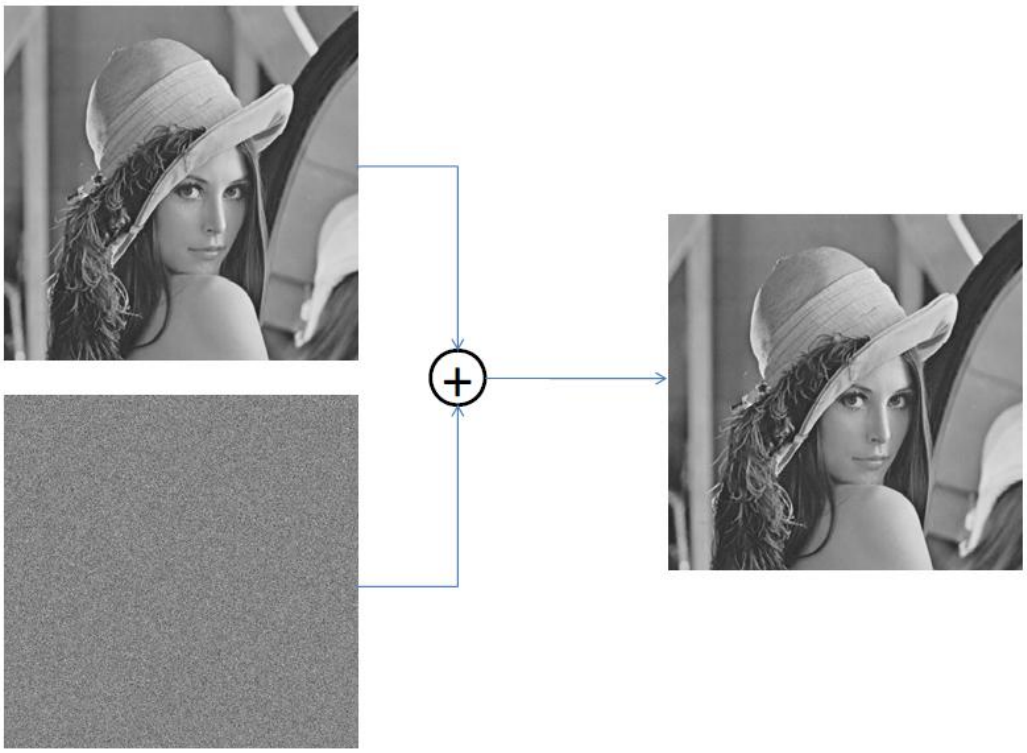
1.1. Информатив эмбеддинг

Ушбу маърузада қўшимча маълумотга асосланган ҳолда қурилган watermarking тизимини қуриш билан яқиндан танишиб чиқилади. Бунинг учун информатив детектор билан ва кейин информатив детектордан фойдаланган ҳолда қўшимча маълумотдан билан қурилган watermarking тизими билан танишиб чиқилади.

Қўшимча маълумотдан фойдаланмаган ҳолда қурилган watermarking тизимида маълумот калит асосида кодланади ва контентга мос ҳолатда келтирилади. Масалан, контент расм бўлса, кодланиш натижасида маълумот контент ўлчамига тенг бўлган расм турида ифодаланади (5.1,5.2-расмлар).



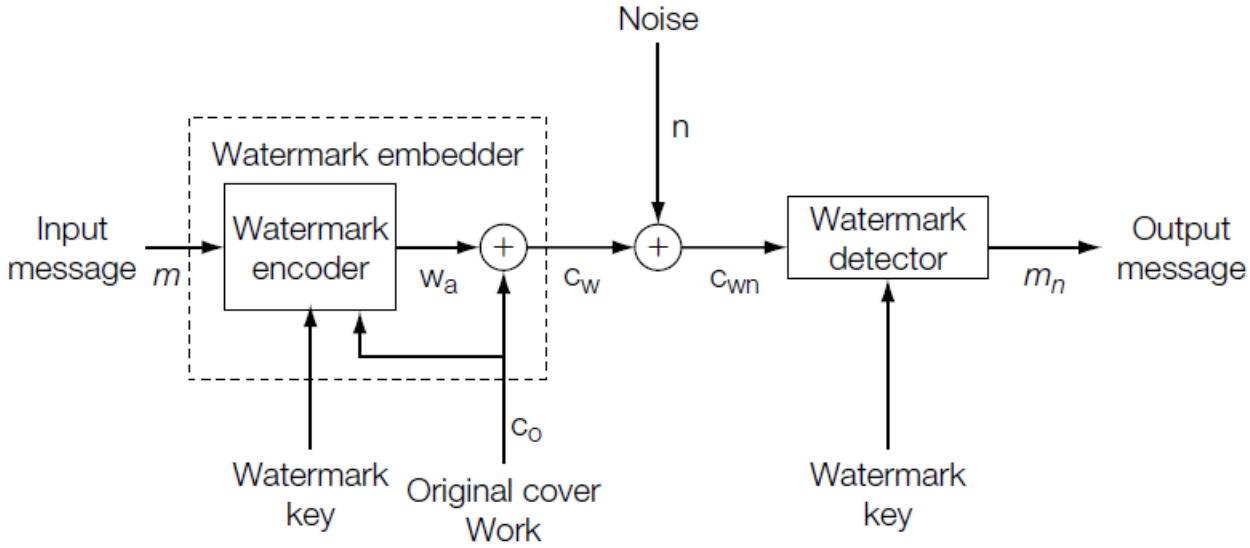
5.1-расм. Қўшимча маълумотдан фойдаланмаган ҳолда watermarking тизими



5.2-расм. Кўркўрона туридаги эмбеддир

Қўшимча маълумотдан фойдаланмаган ҳолда қурилган watermarking тизимида *фойдаланувчанлик* ва *аниқлилик* даражалари катта бўлмаганлиги сабабли, амалда қўшимча маълумотлардан фойдаланган ҳолда қурилган watermarking тизимлари кенг қўлланилади.

Қўшимча маълумотлардан фойдаланган ҳолда қурилган watermarking тизими моделининг умумий кўриниши қуйидагича (5.3-расм):



5.3-расм. Қўшимча канал орқали watermarking тизими

Ушбу келтирилган модель қўшимча маълумотдан фойдаланмасдан қурилган watermarking тизимидан фақатгина ҳақиқий контентдан фойдаланиши билан ажралиб туради.

Watermarking тизими эмбеддер қисмида фақатгина маълумот ва калитдан эмас, балки ҳақиқий контентдан ҳам фойдаланилади. Эмбеддир қисмидан олинган натижа эса контентга бирлаштирилади ва алоқа тармоғи орқали узатилади. Узатилиш давомида ташқи шовқинларнинг қўшили кузатилиб, детектор томонидан қўйилган watermarking маълумотини топиш талаб этилади.

Қўшимча маълумотлардан фойдаланган ҳолда қурилган watermarking тизимларининг *уч турдаги* кўраниши бўлиб, улар: *кўркўрона эмбеддинг усулининг давомчиси*, ва қолган икки тури *dirty-paper кодларига* асосланган усуллардир.

Информатив эмбеддинг ва чизиқли боғланишга асосланган детекторлаш. Бу усул кўркўрона эмбеддинглаш усулининг давомийси саналади. Чунки бу усулда эмбеддинглаш жараёнида контент иштирок этмайди. Шунинг учун уни кўркўрона эмбеддинглаш усулига асосланган дейиш мумкин. Бошқа томондан, эмбеддинглаш жараёнида контент ва маълумот жойлаштирилган қолиб ўртасидаги чизиқли боғланишдан фойдаланилади. Шунинг учун кўркорона эмбеддинглаш давомчиси деб аталади.

Бу усулни тушунтириш учун бир бит маълумот олинган. Бу усулда эмбеддинг ва детекторлаш жараёнлари кетма-кетлиги қуйидагича:

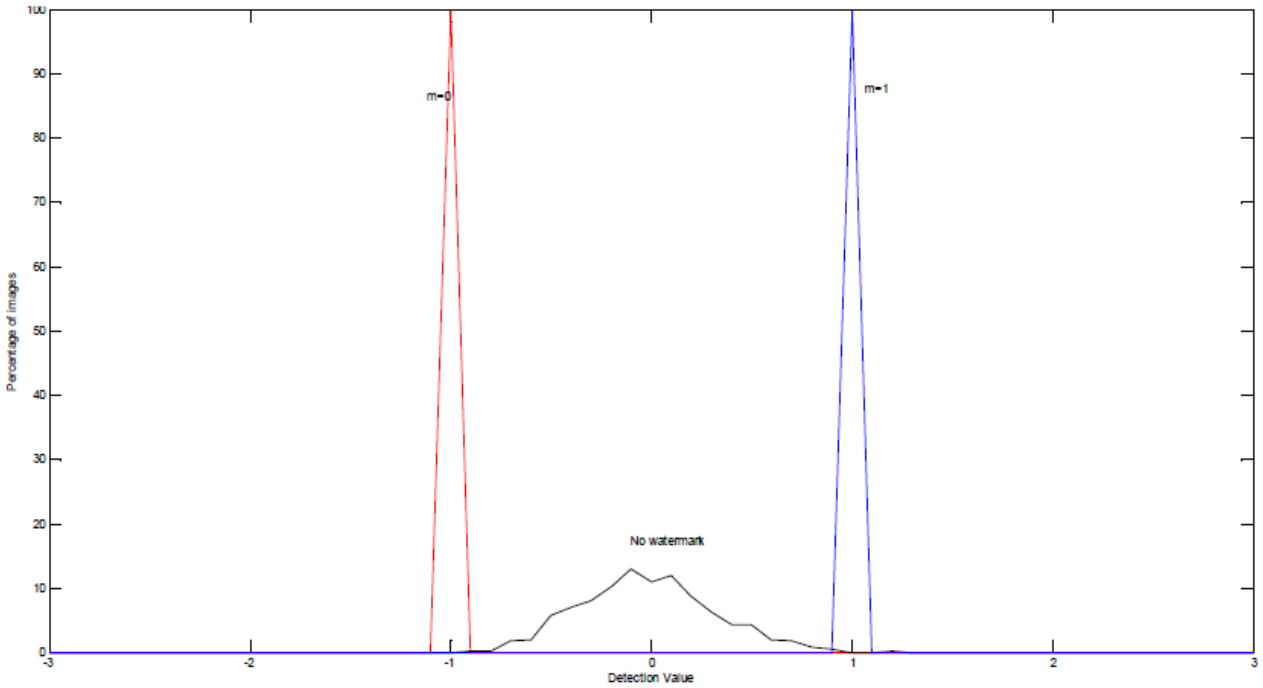
Эмбеддинг жараёни

- Маълумотни жойлаштириш учун тасодифий қолиб олинади (контент ўлчамига тенг бўлган матриц ҳосил қилинади). Бу тасодифий қолипни ҳосил қилишда калитдан фойдаланиш мумкин.
- Ҳосил қилинган қолибга асосан маълумот бити жойлаштирилади. Масалан, маълумот бити бирга тенг бўлса қолиб ҳолати ўзгармайди. Агар маълумот бити нолга тенг бўлса қолибдаги элементлар тескарисига алмаштирилади.
- Шундан сўнг контент ва маълумот жойлаштирилган қолиб орасидаги чизиқли боғлиқлилик, α ҳисобланади. Буни амалга оширишдан мақсад детекторлашда олинган чегара қиймат (threshold) дан катта эканлигини ишонч ҳосил қилиш. Ушбу катталик контентга боғлиқ бўлганлиги сабабли, ҳар бир расм учун турлича бўлади.
- Олинган α қиймат бўйича маълумот жойлаштирилган қолиб масштабланади (контентда жойлаштришда контент сифатини ўзгартириш даражаси).

- Шундан сўнг масштабланган қолиб ва контент бирлаштирилади.

Детекторлаш жараёни:

- Қабул қилинган watermarking қўйилган контент ва калит орқали ҳосил қилинган тасодифий қолиб орасидаги чизиқли боғлиқлилик ҳисобланади.
- Олинган чизиқли боғлиқлилик қийматига кўра маълумот борлиги ёки йўқлиги аниқланади. Агар бу қиймат threshold қийматдан катта бўлса, маълумот бити бирга тенг, агар қиймат threshold қийматининг тескарисидан кичик бўлса, маълумот бити нолга тенг бўлади. Агар олинган қиймат threshold ва тескари threshold қийматлари орасида бўлса, маълумот мавжуд эмас деб топилади.



5.4-расм. Watermarking қўйилган расм учун аниқланган қийматлар

1.2. Dirty-paper кодлари

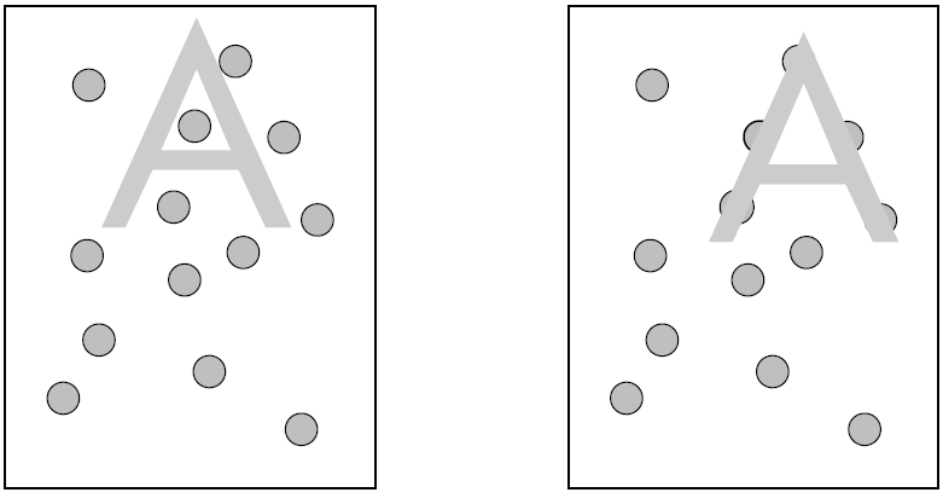
Dirty-paper кодлари бу – кенгайтирилган классик кодлар бўлиб, код сўзларнинг тўплами сифатида ифодаланади. Классик кодларда ҳар бир код сўз ягона хабарни ифодаласа, Dirty-paper кодларида ягона хабар бир нечта код сўзлар тўплами орқали ифодаланади. Шунинг учун Dirty-paper кодларини кодларнинг тўплами сифатида олиш мумкин.

“Dirty-paper” термини дастлаб Макс Костанинг “writing on dirty paper” номли мақоласида келтирилган бўлиб, бунда қуйидагича тасаввур қилинади: “оддий варақда мустақил равишда жойлашган кўплаб нуқталар мавжуд. Бу ҳолда берилган нуқталар орқали хабарни акс эттириш, канал орқали маълумотни юборишга аналогдир. Юборувчига маълумотни қайси

нуқталардан фойдаланган ҳолда акс эттириш маълум, аммо маъумотни ўқувчига бу нарса маълум эмас.” Бундан келиб чиқадики, Dirty-paper деганда мустақил равишда жойлашган нуқталардан иборат бўлган вароқ тушинилади.

Берилган “A” белгисини Dirty-paperда ифодалаш (кўркўрона ва информатив ҳолда) қуйидаги расмда келтирилган (5.5-расм). Watermarking тизими схемасида Dirty-paper ҳақиқий контенга тўғри келиб, белги қўйувчига, эмбеддерга маълум бўлиб, уни текширувчига, детекторга номаълум бўлади. Бунда бир белги учун кўплаб код сўзлар (масалан, A белгисини турли комбинациялар орқали ифодалаш мумкин) тўғри келиши мумкин. Шунинг учун, контентга мос энг мос бўлган код ҳолати олинади.

Dirty-paper кодлари сифати қуйидаги икки хусусиятга боғлиқ бўлади. Биринчи хусусият бу – бир белгини ифодаловчи код сўзларнинг бир-бирига яқинлиги бўлса, иккинчи хусусият эса – турли белгиларни ифодаловчи код сўзлар туркими орасида фарқ катта бўлишидир. Ушбу икки хусусиятни бир-бирига пропорцианал тарзда танлаш Dirty-paper ташкил этишнинг асосий факторидир.



5.5-расм. Dirty-paperда маълумот ёзиш

Қуйида бир бит (1 ёки 0) watermarking маълумоти учун эмбеддинг ва детектор жараёни кетма-кетлиги кўрсатилган.

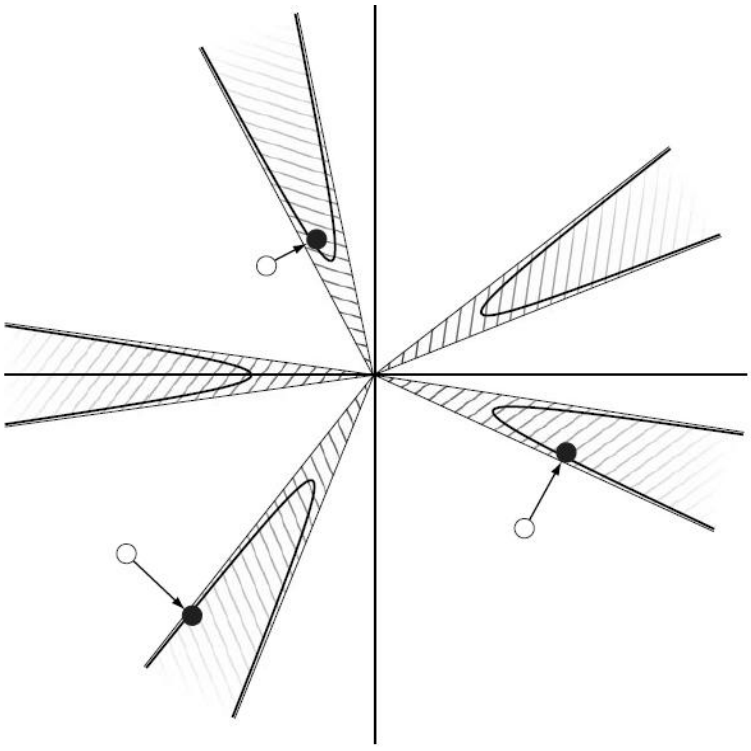
Эмбеддинг жараёни:

- Иккита кодлар тўплами, w_0 ва w_1 (0 ва 1 watermarking маълумотлари учун) контент ўлчамига мос ҳолатда тасодифий сонлар генератори орқали ҳосил қилинади. Бу ерда w_0 нолни ифодалаш учун керакли бўлган кодлар тўплами, w_1 эса бирни ифодалаш учун зарур бўлган кодлар тўпламидир. Генераторнинг дастлабки ҳолати watermarking калити натижасида ҳосил қилинади.

- Нол маълумот битини қўйишда ҳақиқий контендан хусусият вектори ҳосил қилинади. Шундан сўнг ушбу ҳосил қилинган хусусият векторни w_0 тўпламдаги векторлар билан чизиқли боғлиқлилик даражаси текширилади. Энг кўп боғлиқлик мавжуд бўлган тўпламдаги вектор олинади. Шундан сўнг тўпламдан танланган вектор контентга бирлаштирилади. Маълумот бити бирга тенг бўлган ҳолда ҳам худди шунга ўхшаш кетма-кетлик амалга оширилади.

Детектор жараёни:

- Watermarking қўйилган контентдан хусусият вектори ҳосил қилинади. Ҳосил қилинган вектор ва w_0 ва w_1 тўпламдаги векторлар орасидаги чизиқли боғликлилик ҳисобланади. Агар ҳисобланган боғлиқлилик қиймати келишилган чегара қийматдан кичик бўлса, watermarking белгиси мавжуд эмас, акс ҳолда мавжуд. Агар белги мавжуд бўлиб, у w_0 тўпламдаги векторлар билан мувофиқ бўлса, маълумот бити – нолга тенг, агар у w_1 тўпламдаги векторлар билан мувофиқ бўлса, маълумот бити –бирга тенг деб топилади.



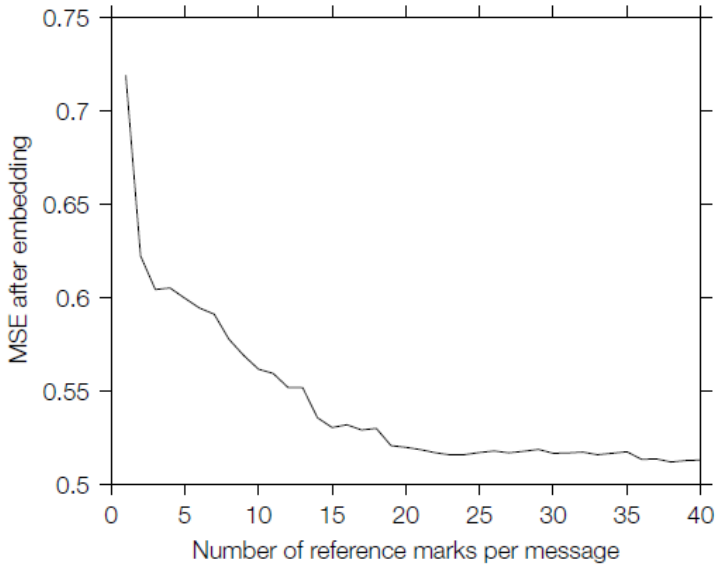
5.6-расм. Детекторлаш жараёни

Юқорида изоҳланган тизим 5.6-расмда кўрсатилган. Бунга асосан штрихланган соҳа детектор орқали текшириладиган бир хабарга тегишли бўлган қисм. Сабаби бир хабар тўплмадаги турли кодлар орқали ифодаланиши мумкин. Яъни, унинг детекторлаш соҳаси бир нечта конуслар тўпламидан иборатдир. Конуслар ичидаги эгри чизиқлар эса ўзгармас аниқлилик даражасидир. Очиқ айланалар белгиланмаган контентни

ифодалайди. Бўйялган айлана ва стрелка эса эмбеддинг жараёнини ифодалаб, очиқ айланани энг яқин детекторлаш соҳасига кўчирилганидир. Ушбу кўчирилишларнинг масофасига қараб тўпламдаги қайси кодга яқинлиги ҳисобланади ва белги топилади.

Ушбу тавсифланган тизимни амалий тарзда қўллаш учун тўпламдаги кодлар сони кичик бўлиши керак. Сабаби катта сондаги кодларни солиштириш ҳар иккала жараёнда, эмбеддинг ва детекторлаш жараёнларига катта ноқулайлик туғдиради.

5.7-расмда ягона маълумот битини w_0 ва w_1 тўпламларда турли сондаги кодлар ва 2.000 га яқин контент билан ифодалашдаги натижалар келтирилган.



5.7-расм. Турли кодлар орасидаги фарқ

Назорат саволлари

1. Қўшимча маълумотдан фойдаланилмаган ҳолда эмбеддинг жараёни.
2. Кўркўрона детектор.
3. Threshold катталиги.
4. Dirty – paper кодлари.

Фойдаланилган адабиётлар

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, (2008). Digital Watermarking and Steganography, the Morgan Kaufmann Series in Multimedia Information and Systems, 2nd Ed.

2. Peter Wayner, (2008). Disappearing Cryptography, Second Edition - Information Hiding: Steganography and Watermarking, Morgan Kaufmann.
3. Bruce Schneier, (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C, second Edition, John Wiley & Sons.

6-маъруза

Хатоликларни таҳлиллаш

Режа:

1. Хабар хатоликлари (message error).
2. Ёлғондан ҳақиқий деб ҳисоблаш (false positive errors).
3. Ёлғондан рад этиш (false negative error).

Таянч иборалар: хабар хатоликлари, ёлғондан ҳақиқий деб ҳисоблаш хатолиги, ёлғондан рад этиш хатолиги.

Жуда яхши тузилган watermarking тизимларида ҳам хатоликлар мавжуд бўлади. Бу маърузада уч турдаги ёлғондан ҳақиқий деб ҳисоблаш, ёлғондан рад этиш ва хабар хатоликлари каби хатоликлар билан танишилиб чиқилади. Келтирилган бу хатолик турлари watermarking тизими фойдаланилган watermarking иловасига боғлиқ бўлади.

Watermarking тизимини шакллантиришда юқорида келтирилган хатоликларни ҳисобга олиш керак. Биринчидан, хатоликларни аниқлаш орқали детекторни аниқлаш чегараси белгиланади. Иккинчидан, олинган хатолик даражаси орқали тизимнинг конфиденциялик даражаси аниқланади.

Фойдаланилган иловалар турига кўра юқорида келтирилган хатоликлар турлича даражада муҳим бўлади. Масалан, ОАВларида ёлғондан рад этиш даражаси юқори бўлса, пул тўлаган шартномачилар ўз рекламаларини телевидениядаги кўра олмайдилар. Агар ОАВ ташкилоти учун, ёлғондан ҳақиқий деб топиш хатолиги муҳим. Сабаби, пул тўланмаган кўрсатув ва рекламаларни намойиш этади.

1.1. Хабар хатоликлари

Хабар хатоликлари детектор хабарни декодлаш жараёнида вужудга келади. Тўғридан-тўғри кодлаш усулида детектор бир хабар аниқланади. Ҳолбуки, бошқа хабар беркитилган бўлади. Кўп белгили хабарларда ҳам декодер томонидан бир ёки бир нечта белгилар хатолик билан аниқланади. Кодлашда бинар алфавитдан фойдаланилган бўлса, хатоликлар *бит хатолик* деб ва *бит хатолик даражаси* деб юритилади.

Хатоликлар умумий ҳолда маълумотга шовқин қўшилиши натижасида ҳосил бўлади. Масалан, белги қўйилган контентдаги турли ўзгаришлар ва ҳак.

Кўп битли ва кўп белгили хабарларни ҳимоялашнинг бир усули бу –

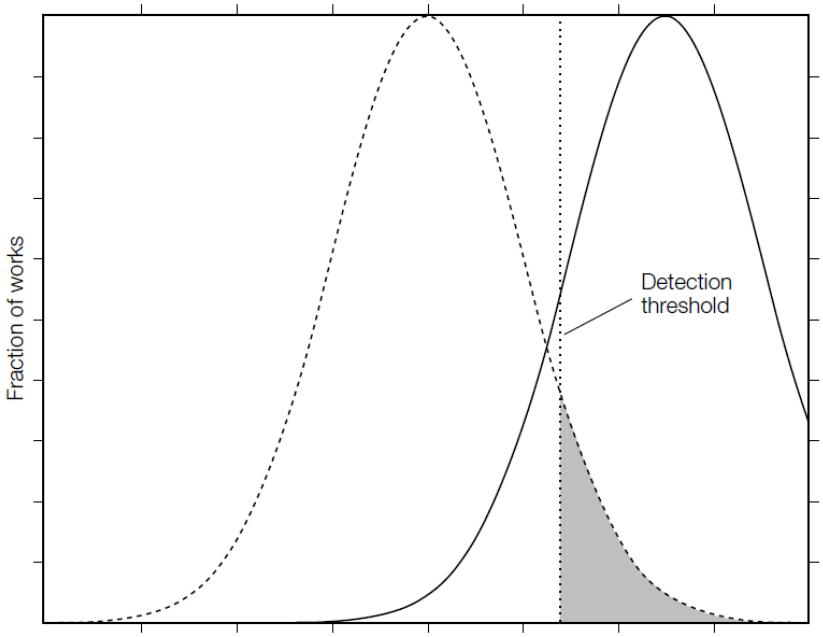
хатоликларни аниқлаш ва тузатиш кодларидан фойдаланишдир. Амалда кўплаб хатоликларни тузатиш ва аниқлаш кодлари кенг фойдаланилади. Бу кодлар икки турга бўлинади. Блокли ва циклик хатоликларни аниқлаш ва тузатиш кодларига ажратилади.

Хатоликларни аниқлаш ва тузатиш кодлари ўзининг максимал аниқлайдиган хатоликлари билан белгиланади. Аниқланган хатолик даражаси турли watermarking тизимига турлича мухим аҳамиятга эга бўлади. Масалан, кўчиришдан ҳимоялаш тизимида *copy-once* хабари мавжуд, яъни хабардан бир марта нусха олса бўлади. Ушбу хабар *copy-freely* тарзда аниқланса, унчалик муаммо бўлмаслиги мумкин. Лекин бу хабар - *never-copy* тарзида аниқланса катта муаммо бўлиши тайин.

Хабарни кодлашда хатоликларни камайтириш учун мавжуд хабарлар орасидаги фарқни иложи борича катта қилиб танлаш аҳамиятга эга.

1.2. Ёлғондан ҳақиқий деб ҳисоблаш

Бу хатолик детектор томонидан watermarking белгиси қўйилмаган контентда watermarking белгиси мавжуд деб кўрсатиши орқали ҳосил бўлади. Агар ёлғондан ҳақиқий деб ҳисоблаш даражаси 10^{-4} га тенг бўлса, бу ҳар 10 000 та детекторлаш уринишида битта хатолик мавжуд бўлишини англатади.



6.1-расм. Ёлғондан ҳақиқий деб ҳисоблаш даражаси (белгиланган соҳа)

Юқоридаги расмда келтирилган, чап томондаги эгри чизиқ watermarking белгиси мавжуд бўлмаган контентдан детектор томонидан аниқланадиган белгиларни такрорланиш частотаси. Шунга ўхшаш ўнг томондаги эгри чизиқ эса, watermarking белгиси мавжуд бўлган контентдан

детектор томонидан аниқланадиган белгиларнинг частотаси. Вертикал узиқ чизиқлар эса аниқлаш чегарасини билдиради. Агар детектор қиймати аниқланиш чегарасидан кичик бўлса, watermarking белгиси мавжуд эмас. Катта бўлган ҳолда эса мавжуд деб топилади. Ёлғондан ҳақиқий деб топиш хатолиги мавжуд бўлиши тайин. Сабаби, аниқлаш чегарасидан катта бўлган тақдирда ва тенг бўлган тақдирда расмда кетлирилган белгиланган соҳа мавжуд бўлади. Ушбу белгиланган соҳа ёлғондан аниқлаш даражасини билдиради. Шунинг учун аниқланиш чегарасини ортириш натижасида, ёлғондан аниқлаш даражаси камайса, бошқа томондан ёлғондан рад этиш даражаси кўпаяди.

Ёлғондан ҳақиқий деб топиш модели детектор алгоритмига боғлиқдир. Хусусан, детектор бир контентдан кўп белгиларни аниқлаш учун, кўп контентлардан бир белгини аниқлаш учун ёки кўп контентдан кўп белгини аниқлаш учун фойдаланилиши мумкин. Биринчи ҳолда, watermarking белгисини тасодифий ўзгарувчи бўлади. Иккинчи ҳолда, watermarking белгиси мавжуд контент тасодифий ва ҳар иккала катталиклар тасодифий бўлади. Бу эса ўз навбатида *тасодифий-watermarking ёлғондан ҳақиқий деб топиш* ва *тасодифий-контент ёлғондан ҳақиқий деб топиш* консепциясини келтириб чиқаради.

Масалан, кўчиришдан назоратлаш тизими бир watermarking белгисини миллионлаб контентлардан қидирашга тўғри келади. Бу ҳолда олинадиган ёлғондан ҳақиқий деб топиш катталиги қўйилган watermarking белгисига ва белги қўйилмаган ҳолдаги контентга боғлиқ бўлади (*тасодифий-контент ёлғондан ҳақиқий деб топиш*). Бошқа томондан эса, DiVX иловаларида, миллионлаб DiVX плейерларда ҳар бири билан уникал бўлган watermarking белгиси мавжуд бўлади. Бу тизим ноқонуний кўчиришдан ҳимоялаш учун, бир видео контент ичидан миллионлаб watermarking бедгисини қидиришга тўғри келади.

Тасодифий-watermarking ёлғондан ҳақиқий деб топиш. Бу ҳолда қўйиладиган watermarking белгилари ўзгарувчан, кўп бўлиб, контент эса ягона ўзгармас катталикдир (6.2-расм).

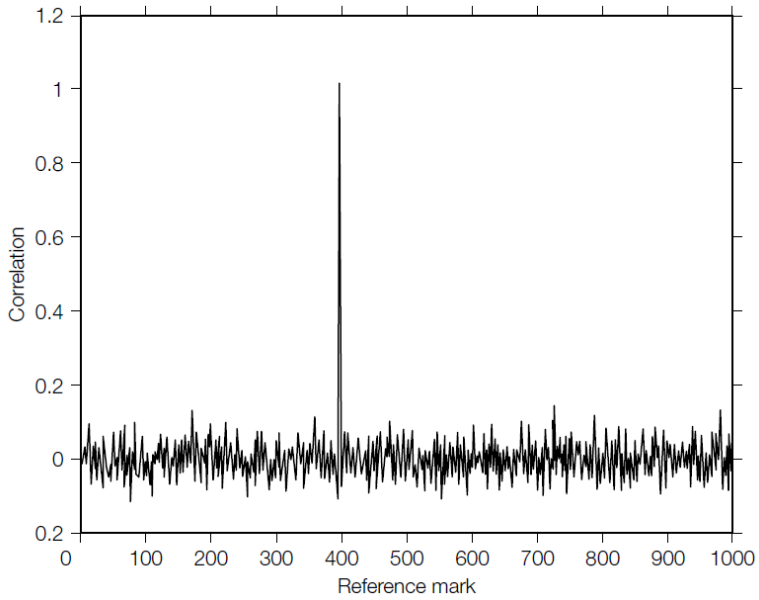
Тасодифий-контент ёлғондан ҳақиқий деб топиш. Бу ҳолда минглаб контентлардан бир хабар маълумот қидирилади. Шунинг учун бу вазиятда контент тасодифий ва белиги эса ўзгармас деб олинади.

1.3. Ёлғондан рад этиш

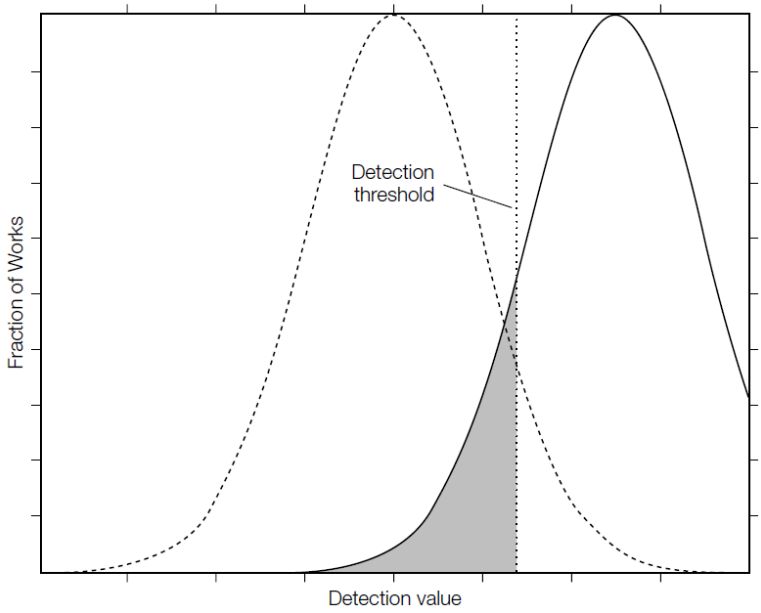
Бу хатолик watermarking белги мавжуд бўлган контентдан детектор

орқали белги мавжуд эмас деб топилиши. Бу ҳолат *ёлғондан рад этиш даражаси* деб номланган катталик билан белгиланади. Ёлғондан рад этиш даражаси 6.3-расмда акс эттирилган. Расмдаги ўнг томонда жойлашган эгри чизиқнинг аниқлаш чегарасидан кичик бўлган белгиланган соҳаси ёлғондан рад этиш даражасини кўрсатади.

Ёлғондан рад этиш даражаси ҳар иккала ҳолат, белгини қўйиш ва уни аниқлаш жараёнларини қанчалик аниқлик даражасида бажарилишига боғлиқ.



6.2-расм. Тасодифий-watermarking ёлғондан ҳақиқий деб топиш



6.3-расм. Ёлғондан рад этиш даражаси

Белги қўйилган контент узатилиш жараёнида кўплаб ўзгартиришларга учраши мумкин. Бунинг натижасида ёлғондан рад этиш даражаси ортиб боради. Бундан ташқари кўплаб бузғунчилар белги мавжуд контент устида

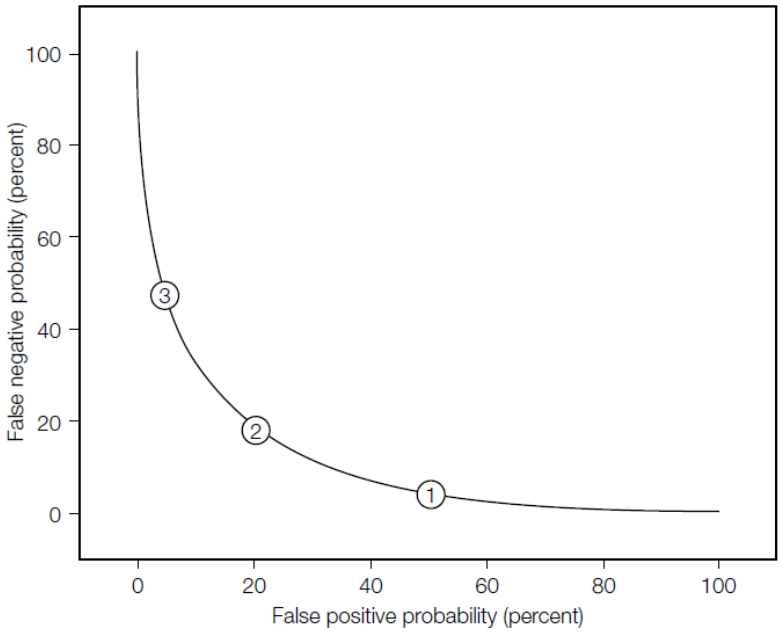
турли ўзгартиришларни амалга оширади. Бунинг натижасижа бу кўрсаткич хаттоки 100 % гача этиши мумкин. Шунинг учун ёлғондан рад этиш даражасини ҳисоблашдан олдин эмбеддинг ва детектинг жараёнлари орасида қандай жараёнлар бўлиши мумкинлигини аниқлаш керак.

Бўлиши мумкин бўлган жараёнларни умумий ҳолда уч турга ажратиш мумкин:

Хавфсизликга оид. Биринчи ҳолат бу бузғунчи томонидан белги қўйилган контентдан рухсат этилмаган ўчириб ташлаш орқали белгини аниқлаб бўлмас ҳолда келтириш. Бу ҳолда ёлғондан рад этиш даражаси кўпаяди. Тизим хавфсизлиги $1\text{-}P_{fn}$ га тенг бўлади. Бу ерда P_{fn} ёлғондан рад этиш кутилмаси.

Чидамлиликга оид. Иккинчи ҳолат белги қўйилган контентни турли ўзгаришларга учраши (турли ўзгартиришлар, сиқилашлар ва ҳак.) натижасида ёлғондан рад этиш даражасини ортишидир. Бу ҳолда чидамлилик $1\text{-}P_{fn}$ га тенг бўлади.

Эффективлигига оид. Бу ҳолат эмбеддинг ва детектор жараёнлари орасида ҳеч қандай бузулиш бўлмаган ҳолни ифодалайди. Бу ҳолда тизим эффективлиги $1\text{-}P_{fn}$ га тенг бўлади.



6.4-расм. Ёлғондан рад этиш ва ёлғондан тасдиқлаш кўрсаткичлари орасидаги боғланиш

Назорат саволлари

1. Хабар хатоликлари.
2. Ёлғондан тасдиқлаш кўрсаткичи.
3. Ёлғондан рад этиш кўрсаткичи.

Фойдаланилган адабиётлар

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, (2008). Digital Watermarking and Steganography, the Morgan Kaufmann Series in Multimedia Information and Systems, 2nd Ed.
2. Peter Wayner, (2008). Disappearing Cryptography, Second Edition - Information Hiding: Steganography and Watermarking, Morgan Kaufmann.
3. Bruce Schneier, (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C, second Edition, John Wiley & Sons.

7-маъруза

Сезилувчан моделлардан фойдаланиш

Режа:

1. Сезилувчанлик ва унинг турлари.
2. Сезилувчанликни аниқлаш усуллари.
3. Сезилувчан моделларнинг умумий кўриниши.

Таянч иборалар: Сезилувчанлик, аниқлилик, сифат, автоматик аниқлаш, частота сезилувчанлиги, ниқоблаш, бирлаштириш.

1.1. Сезилувчанлик ва унинг турлари

Watermarking тизимларининг муҳим бир хусусияти бу қўйилган белгининг сезилмаслигидир. Бу эса ўз навбатида қандай қилиб белгини сезиларлилик даражасини аниқлаш мумкин ва қандай қилиб белгиларни сезилмас қилиб яшириш мумкин деган саволларни келтириб чиқаради. Бу маърузада юқоридаги саволларга жавоб бериш учун сезиларли моделлардан қандай қилиб фойдаланиш тартиби келтирилган.

Аниқлилик ва сифат. Сигналларга ишлов бериш тизимларида икки турдаги сезилувчанлик ажратилади: *аниқлилик* ва *сифат* сезилувчанлиги. Аниқлилик бу жараёндан олдинги ва кейинги контентнинг ўзгаришидаги фарқни кўрсатади. Агар белги қўйилган ва қўйилмаган контент орасида фарқ қанча катта бўлса аниқлилиқ шунча паст, қанча кичик бўлса аниқлилик шунча катта бўлади. Шунга қараб моделнинг сезилувчанлик даражаси белгиланади. Бошқа томондан сифат хусусияти контентнинг абсолют хусусияти бўлиб, расмнинг юқори сиқатлигини, аудио ёзувни яхшилини билдиради. Икки турдаги сезилувчанлик ҳам watermarking тизимларини баҳолашда кенг фойдаланилади.

Аниқлилик ва сифат хусусиятларини бир-биридан фарқини ажратиш учун камерадан келаётган видео кетма-кетликни олиш мумкин. Видео маълумот грейскейл, сиқилган, умуман олганда сифати паст бўлиши мумкин. Аммо шундай вазиятда ҳам унга watermarking белгиси қўйилса асл контентдан фарқ қилмаслиги мумкин, юқори аниқлилик даражасига эга. Амалда юқори даражали сифатга эга ва паст даражали аниқлилик даражасига эга тизимлар ҳам учрайди.

Иловалар турига қараб аниқлилик юқори бўлиши ёки сифат биринчи даражали бўлиши мумкин.

1.2. Сезилувчанликни аниқлаш усуллари

Сезилувчанликни инсон томонидан аниқланиши. Кўплаб watermarking тизимларида контентлар орасидаги фарқни аниқлашда автоматилашган усуллардан фойдаланилса, баъзи тизимларда инсон қобилятидан фойдаланилади. Инсонларнинг белгиларнинг ажратиш қобиляти булар орасида тенг бўлмайди. Икки расмдаги фарқни турли инсонлар турлича аниқлаши мумкин. Мусиқа соҳасида яхши қобилятга эга инсонлар "*олтин қулоқ"* соҳиблари деб аталса, кино соҳасида эса *"олтин кўзлар"* деб аталадилар.

Психологик томондан икки контентдаги ўзгаришларни 50 % ни аниқлаш *шунчаки кўринарли фарқлар* деб аталади. Инсонлар орқали контентлар орасидаги фарқни аниқлашда *икки вариантли мажбурий танлов (two alternative, forced choice (2AFC))* усулидан фойдаланилади. Масалан, контентнинг сифат фарқини аниқлаш талаб этилса, иштирокчиларна иккита контент, ҳақиқий ва белги яширинган кўринишлар тақдим этилади. 2AFC усули контентлардаги аниқлилик фарқини аниқлашда фойдаланилса, унда учта контент тақдим этилади. Биринчиси, ҳақиқий контент, иккинчиси контентдан нусха ва учунчиси белги яширинган контент. Бунда иштирокчидан кейинги икки контентдан қайси бири биринчи контентга ўхшашлигини аниқлаш талаб этилади.

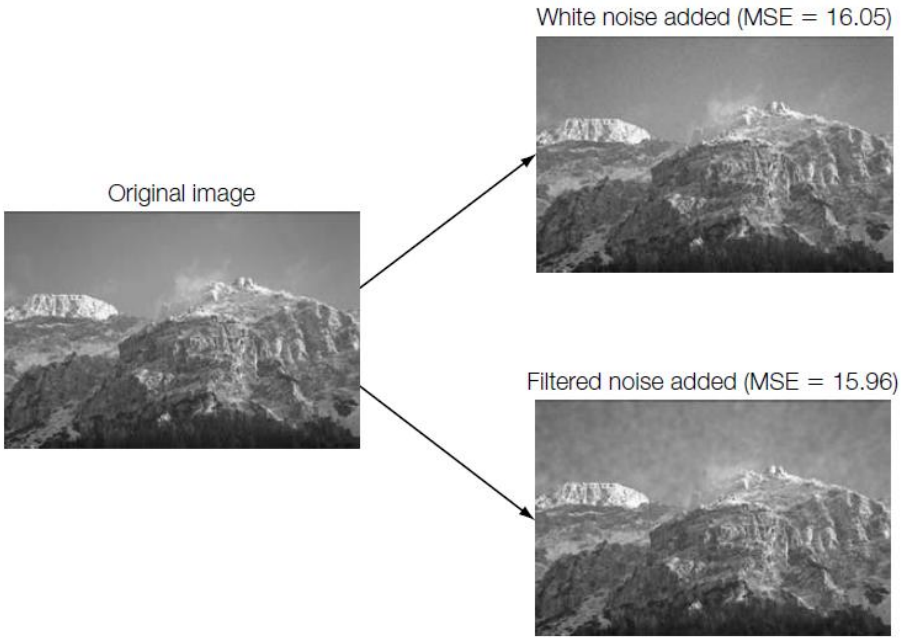
Автоматик аниқлаш. Амалиётда инсон иштирокида аниқлиликни ва ҳаттоки сифатни жуда яхши аниқлаш имкони мавжуд эмас. Бундан ташқари фойдаланилаётган кўплаб тизимларда аниқлилик кўрсаткичини топиш талаб этилади. Ҳаттоки жуда катта аниқлилик даражаси ҳам сифатни озгина бўлсада ўзгаришига олиб келади.

Шундан келиб чиқиб, инсон ёрдамида топилган аниқлилик ва сифат ўзгаришидан яхшироқ натижани амалиёт талаб этади. Шунинг учун амалиётда автоматик аниқлаш усулларидан кенг фойдаланилади.

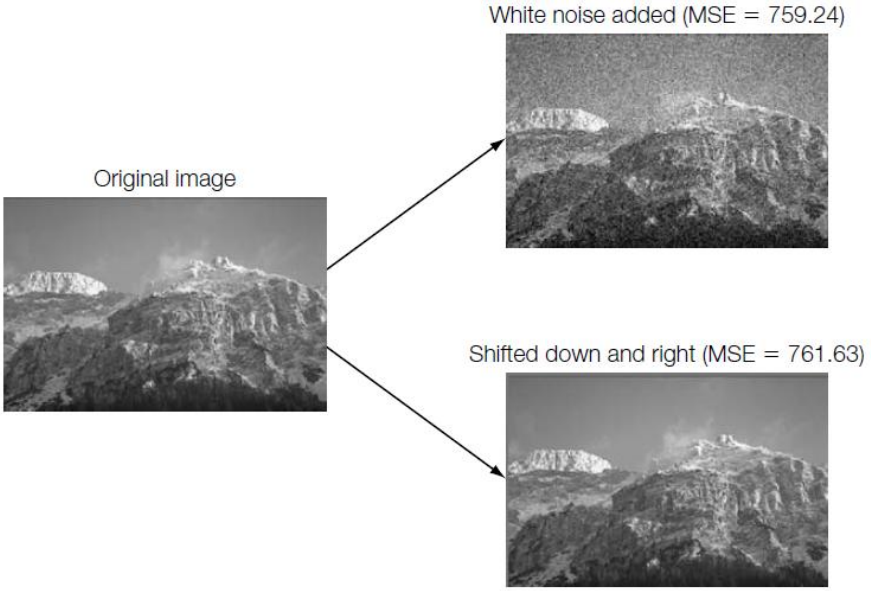
Сезилувчан модел тушанчасини одатда икки, ҳақиқий контент, c_0 ва watermarking белгиси мавжуд, c_w контент орасидаги $D(c_0, c_w)$ қиймати қанчалигига қараб аниқланади. Ушбу қийматни содда ҳисоблаш усулларидан бири бу *ўртача квадратик хатолик* бўлиб, қуйидагича ифодаланади:

$$D_{mse}\ c_0, c_w\ = \frac{1}{N} \sum_{i}^{N} (c_w\ i\ - c_0[i])^2$$

Қуйидаги мисолда турли ҳоллардаги MSE уёрдамида олинган натижалар келтирилган.



7.1-расм. MSE хатолигига мисол



7.2-расм. MSE хатолигига мисол

7.2-расмда ҳақиқий рамнинг икки ўзгариши келтирилган. Биринчисига оқ шовқин қўшилган ва MSE қиймати 759.24 га тенг. Иккинчи ҳолат ҳақиқий расмнинг ўнга ва пастга силжитилган кўриниши бўлиб, у учун MSE қарийиб биринчи ҳолатга яқин. Бу эса MSE усулининг контентларни турли айлантириш ҳолатлари учун бардошсиз эканлигини англатади.

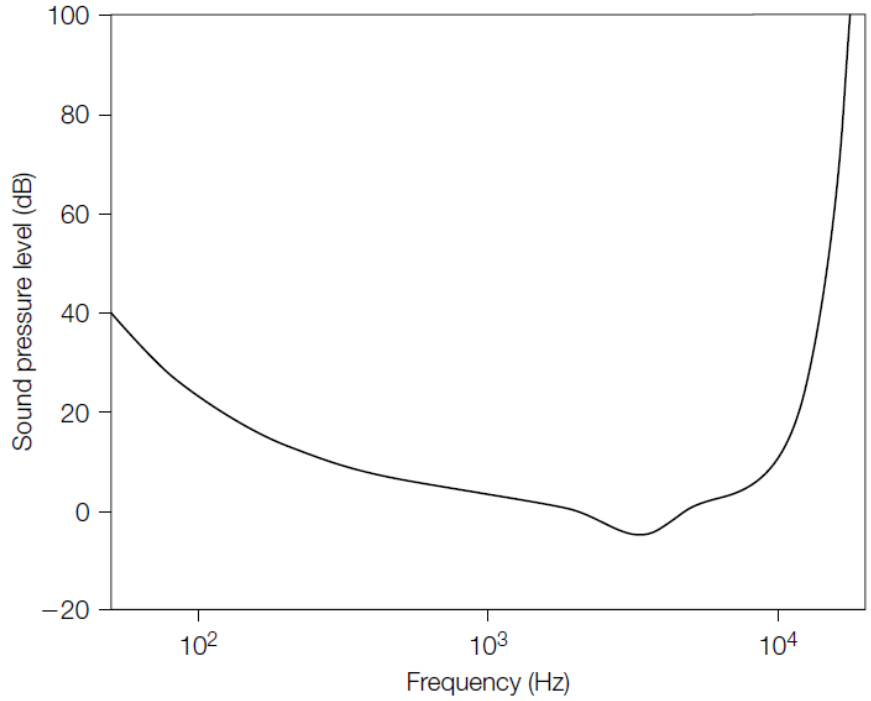
1.3. Сезилувчан моделларнинг кўринишлари

Сезилувчан моделлар қуйидаги уч: *сезувчанлик, ниқоблаш* ва *бирлаштириш* ҳолатларида бўлиши мумкин.

Сезилувчанлик. Сезувчанлик бу инсон кўзлари ва қулоқлари

томонидан бир қарашда билинадиган хусусиятларга нисбатан ишлатилади. Бу хусусиятлар аудио ёзувлар учун частота ва қаттиқлик, расмлар учун ёркинлик бўлиши мумкин. Бундан ташқари расм ва видео маълумотлар учун ранг ва ориентациялар сезилувчан хусусиятлар бўлиши мумкин.

Частота сезилувчанлиги. Овозларни эшитилишида турли частоталар турли тонларда қабул қилинади. Қуйидаги 7.3-расмда инсон эшитиш сезувчанлигини частоталарга боғлиқлиги графиги келтирилган. Бу графикка кўра инсон қулоқлари 3 kHz частота атрофида жуда сезилувчан бўлиб, сезилувчанлик 20 Hz га қадар камайиб боради ва 20 kHz да жуда юқори бўлади.



7.3-расм. Эшитишнинг сезилувчанликка таъсири

Ниқоблаш. Ҳолат сезилувчанликка таъсир этади. Баъзида белгиланган тонни аниқлаш имконияти, ёнидаги тон частотаси натижасида йўқолиши мумкин. Масалан, 7.4 - расмда ҳақиқий расм ва бир хил шовқин қўшилган кўриниши берилган.

(a) Original

(b) Watermarked

7.4 – расм. ҳақиқий ва бир хил шовқин қўшилган расм ҳолати

Юқоридаги расмда шовқин бир хил бўлсада, ҳақиқий расмга қўшилганда уни бир хил ўзгартирмади. Бунинг сабаби ҳақиқий расмнинг турли соҳаларда ранглари турлича бўлишидир. Б ҳолатдаги расмнинг осмон қисмида шовқин қўшилганлиги яққол кўринади.

Бирлаштириш. Сезилувчанлик ва ниқоблаш хусусиятлари контентнинг аниқ бир хусусияти ўзгарганлигини аниқлашда фойдаланилади, масалан ягона частота ўзгариши. Бундан ташқари, кўп частоталар ўзгарса, сезилувчанлик ва ниқоблашни барча частоталар бўйича ҳисоблашга тўғри келади. Ягона контент бўйича турли ўзгаришларини ягона ҳисобини берувчи катталикка *бирлаштириш* деб аталади. Бирлаштириш қуйидаги формула билан ифодаланади:

$$D\ c_0, c_w\ = (\sum_i |d[i]|^p)^{\frac{1}{p}}$$

Бу ерда $d[i]$ катталик c_0, c_w векторлар орасидаги бир параметр бўйича ўхшашлик даражасини аниқлайди. Юқоридаги тенглик Минровски йиғиндиси деб аталади. Контент аудио бўлган ҳолда $p=1$ га ва контент расм бўлган ҳолда $p=4$ га тенг деб олинади.

Назорат саволлари

1. Сезилувчанлик, аниқлик ва сифат.
2. Сезилувчанликни инсон томонидан аниқлаш.
3. Автоматик аниқлаш.
4. Сезилувчанлик моделлари.

Фойдаланилган адабиётлар

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, (2008). Digital Watermarking and Steganography, the Morgan Kaufmann Series in Multimedia Information and Systems, 2nd Ed.
2. Peter Wayner, (2008). Disappearing Cryptography, Second Edition - Information Hiding: Steganography and Watermarking, Morgan Kaufmann.
3. Bruce Schneier, (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C, second Edition, John Wiley & Sons.

8-маъруза

Бардошли watermarking

Режа:

1. Бардошли watermarking тизимларини қуриш усуллари.
2. Бардошли watermarking тизимларига таъсирлар.

Таянч иборалар: бардошли watermarking, таъсирлар, вақтинчалик таъсирлаш, геометрик таъсирлар.

Кўплаб иловалар watermarking белгиси қўйилгандан сўнг контент ўзгаришларга учраган тақдирда ҳам белгини аниқланишини талаб этади. Бундай талабларга жавоб берадиган тизимлар *бардошли watermarking* тизимлари деб аталади. Ушбу бўлимда бардошли watermarking тизимларини қуришни баъзи усуллари ва жараёнлари ҳақида тўхталиб ўтилади.

Watermarking тизимларининг бардошлиги ва хавфсизлиги турли хусусиятлар бўлиб, бардошли watermarking тизимлари нормал жараёнларга қарши тура олиш қобиляти саналса, хавфсиз watermarking тизимлари бузғунчи томонидан қилинган ҳужумларга қарши тура олиш қобилятини белгилайди. Ушбу хусусият бир –бирига боғлиқ бўлиб, тизим хавфсиз бўлиши учун у бардошли бўлиши талаб этилади. Аммо, бардошли бўлишни ўзи тизим хавфсиз бўлиши учун етарли бўлмайди. Шунинг учун тизим яратувчиси яратилаётган watermarking тизимини барча таҳдидларга қарши тура олишни таъминлаши шарт. Ушбу маърузада тизимнинг бардошлилик хусусияти таҳлил этилса, кейинги маърузада тизимнинг хавфсизлик хусусияти таҳлил этилади.

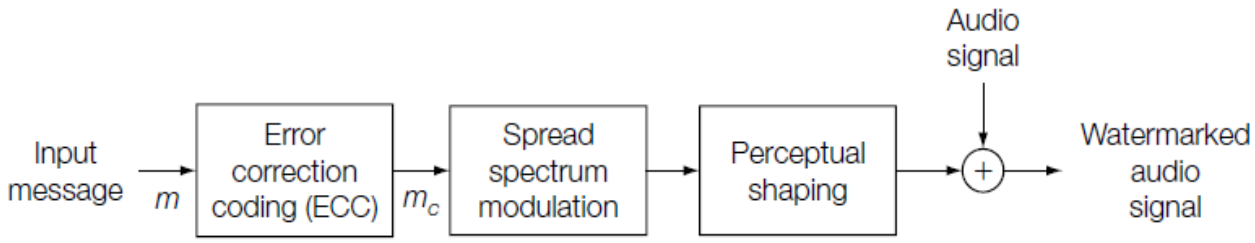
1.1. Бардошли watermarking тизимларини қуриш усуллари

Амалда белги мавжуд контент маълум ўзгаришларга учраган тақдирда ҳам белгини топиш имконияти мавжуд. Бу иш одатда белги мавжуд контент элементларини сақлашга қаратилган бўлади. Бошқа усулларда эса белги мавжуд контент маълум турдаги бузулишларга қарши қилиб ишлаб чиқилади. Амалда белги мавжуд контентда турли ўзгартиришларга бардошли бўлиши керак. Қуйида бардошлилик хусусиятини таъминлаш усуллари таҳлил этилади.

Қолдиқ маълумот қўшиш. Одатда белги мавжуд контент турли ўзгаришларга учраганда, ўзгариш контент юзаси бўйлаб текис тақсимланмайди. Бошқа сўз билан айтганда, ўзгартириш контентнинг маълум қисмига ёки маълум юзасига тасир этади. Қолган қисмлар эса ўзгиришсиз

сақланиб қолади. Бу ҳолда белги мавжуд контентни бардошлилигини таъминлаш усули унга қўшимча *қолдиқ маълумот қўшишдир.* Қўшилган қолдиқ белги маълумотлари асосида ҳисобланади. Агар контентдаги ўзгаришлар натижасида белгининг маълум қисми ўзгарса, ўзгармаган қисми орқали уларни тиклаш имконияти мавжуд бўлади. Бу усулда одатда хатоликларни тузатиш кодларидан кенг фойдаланилади. Ўзгартирилган маълумотни қайта тикланиш даражаси хатоликларни тузатиш кодлари имконияти билан ўлчанади.

Кенг поласали спектрум кодлаш. Агар частоталар соҳасидан фойдаланилганда (аудио сигналларда), қолдиқ маълумот қўшиш усули янги кенг поласали спектрум кодлаш усулини келтириб чиқаради. Бу усулда маълумот нол ва бирлардан иборат бўлган кетма-кетлик ҳолатига келтирилади. Шундан сўнг контент (аудио сигнал) кенг поласалар бўйлаб тарқатилади ва маълумот битлари бу поласалар узра тенг ёйилади. Узатилиш давомида маълум частоталарда ўзгариш бўлган тақдирда ҳам, бошқа частоталарда маълумот битлари сақланиб қолади. Сақланган маълумот битларидан хатоликларни тузатиш кодлари орқали йўқотилган маълумот битлари тикланади.



8.1 – расм. Содда кенг поласали спектрум кодлаш усули

Ўзгарувчанликка бардошли саналган коэффициент ўрнига қўйиш усули. Амалда хабар маълумотни контентнинг барча коэффициентлари ўрнига яшириш тўғри саналмайди. Сабаби, контентнинг баъзи коэффицентлари ўзгаришларга бардошсиз саналади. Масалан, расм типидаги контентлар Фуре кўринишидаги юқори частоталари ўзгаришларга бардошсиз бўлиб, одатда ўзгаришлар шу қисмларга катта таъсир қилади. Бу эса ушбу соҳада маълумотни яшириш мумкин эмаслигини келтириб чиқаради.

Бу усул контент юзасини ўзгарувчанликка бардошли саналган ва бардошли саналмаган қисмларга ажратиш ва уларда маълумот битларини яширишга асосланган. Ўзгарувчанликка бардошли саналган қисм маълумот яширишга мос бўлиб, унда яширинган маълумот ўзгаришларга бардошли бўлади. Аксинча, бардошли саналмаган қисмларга маълумот битларини яшириш уларни ўзгаришларга учраганда ўзгаришига олиб келади.

Ушбу усулнинг мураккаблиги шундаки, ўзгарувчанликка бардошли саналган қисмларга маълумотни яшириш контентнинг ўзгаришига катта тасир қилади. Ўзгаришга бардошли саналмаган қисмлар контент ўзгаришига катта таъсир этмасада, уларда маълумотни яшириш ўзгаришларга таъсирли бўлади. Масалан, муҳимлиги кам саналган битлар ўрнига маълумотларни яшириш усулидан фойдаланилганда, яширинган маълумот контент ўзгаришига катта таъсир қилмасада, бу усулда белгили контент ўзгаришларга таъсирли саналади. Содда мисол сифатида олинса, расм пиксели 202 га тенг. Агар бу расм ўзгаришга учраган тақдирда уни 201 ёки 203 га ўзгариши уни 2 га ўзгаришига қараганда кўпроқ эҳтимолликка эга.

Белгиланган бардошлиликка эга коэффицентлар ўрнига қўйиш. Юқоридаги усулда контент бўлиши мумкин бўлган барча ўзгаришларга қарши бардошли саналади. Аммо, амалда кўплаб тизимлар фақат белгиланган ўзгаришларга бардошли қилиб ишлаб чиқилади. Масалан, watermarking тизимининг мақсадидан келиб чиқиб, унга бўлиши мумкин бўлган ўзгаришлар ўрганилади ва тизимни ишлаб чиқишда ушбу ўзгаришларга қарши усуллардан фойдаланилади.

Белгиланган бардошлиликга эга коэффицентлар ўрнига қўйиш усулида ишлаб чиқилган тизимдаги эмбеддер ва детекторга керакли бўлган контентдаги маълум коэффицент (масалан, пикселдаги белгиланган бит ўрни) ўрнига маълумот бити қўйилади. Юқоридаги усулда аниқ белгиланган коэффицент ўрнига маълумот битлари қўйилса, бу усулда ҳар бир контент хусусиятидан келиб чиққан ҳолда ундан маълум коэффицентлар танланади ва уларнинг ўрнига маълумот битлари қўйилади.

Детекторда ўзгаришларни инвертлаш. Юқоридаги кўриб ўтилган барча усуллар қўйилган белгини турли ўзгаришларга бардошли бўлишини таъминлайди. Бу усулда эса эмбеддинг жараёнида амалга оширилган бирор жараённи детектор томонидан инвертлашга асосланади. Кўплаб жараёнлар аниқ ёки қисман инвертланиши талаб этилади. Масалан, эмбеддинг жараёнида расм соат стрелкаси йўналишида айлантирилса, детекторлаш жараёнида расм соат стрелкаси йўналишига тескари ҳолда айлантирилади. Агар эмбеддинглаш ва детекторлаш оралиғида контентга бирор жараён амалга оширилса, у ҳолда детектор қисман инвертлашни амалга оширади.

Алтернатив ҳолда, watermarking алгоритмларига боғлиқ ҳолда детектор томонидан инвертлаш бутун белги қўйилган контентдаги ўзгаришлар бўйича эмас, балки, фақат белгилар соҳаси бўйича амалга оширилади. Бу ҳолда детектор томонидан инвертлаш учун сарфланидаган қувват ва вақт тежаб қолинади.

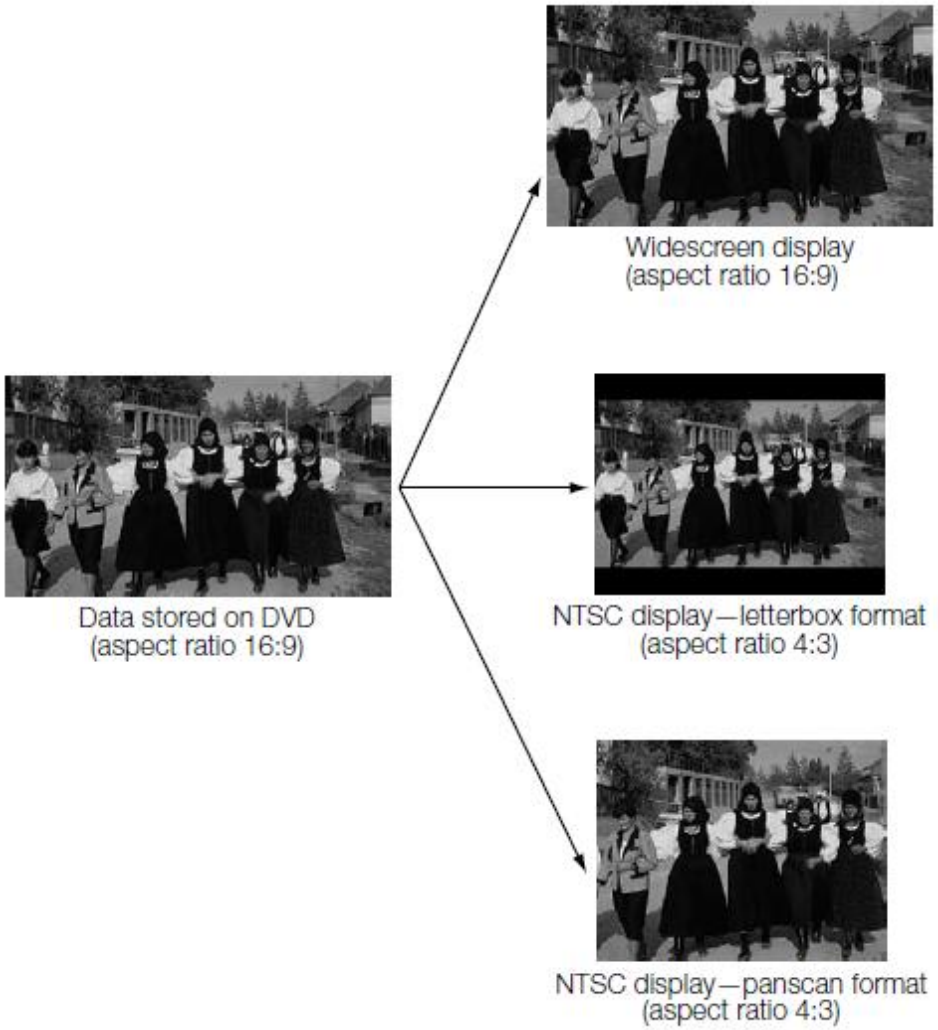
Ўзгаришларни инвертлашдаги қийин қадамлардан бири бу қайси

ўзгаришни инвертлаш кераклигини аниқлашдир. Кўплаб ҳолларда афсуски, детектор барча ўзгаришларни инвертлаб, кейин белгини тестлаш орқали аниқлайди.

Ўзгаришларни аниқлаш кўркўрона детекторларга қараганда информатив детекторлар учун осонроқ бўлиб, бу ҳақиқий контент ва белги қўйилган контент орасидаги ўзгаришларга кўра аниқланади.

Эмбеддерларда олдиндан инвертланган ўзгаришлар асосида. Баъзи тизимларда белги қўйилган контентга бўлиши мумкин бўлган ўзгаришлар олдиндан маълум бўлади. Масалан, видео маълумотларни ўқувчи DVD қурилмаси фойдаланувчи талабларига асосан high-definition television (HDTV) (расм ўлчами 16:9), NTSC ва PAL (расм ўлчамлари 4:3) стандартларини ўқиш имкониятига эгалиги айтилган бўлсин (8.2-расм). Агар watermarking белгиси widescreen (16:9) ҳолати учун қўйилган бўлса, унда детектор бу ҳолатдаги контентдан белгини аниқлай олади. Аммо, NTSC ва PAL ҳолатлари учун у белгини аниқлай олмайди. Сабаби, ушбу ҳолатда ўтказиш учун контентга турли геометрик ўзгаришлар олиб борилади.

Демак, юқоридаги ҳол учун ҳақиқий контентдаги белгини икки ҳолат NTSC ва PAL стандартига ўтказилган ҳолда ҳам ўзгармаслиги талаб этилади. Бунинг учун эса NTSC ва PAL стандартига ўтказишда қўйилган белгига таъсир этмайдиган геометрик ўзгаришларларни амалга оширишнинг ўзи этарли. Бошқа сўз билан айтганда, *Эмбеддерларда олдиндан инвертланган ўзгаришлар асосида* бардошлиликни таъминлашда олдинган бўлиши мумкин бўлган ўзгаришлар аниқланади ва қўйилган белгини ушбу ўзгаришларга қарши тура олиши таъминланади.



8.2 – расм. DVD да мавжуд уч турдаги файл турлари

Эмбеддерларда олдиндан инвертланган ўзгаришлар асосида бардошлиликни таъминлашда қуйидаги учта босқичдан фойдаланилади:

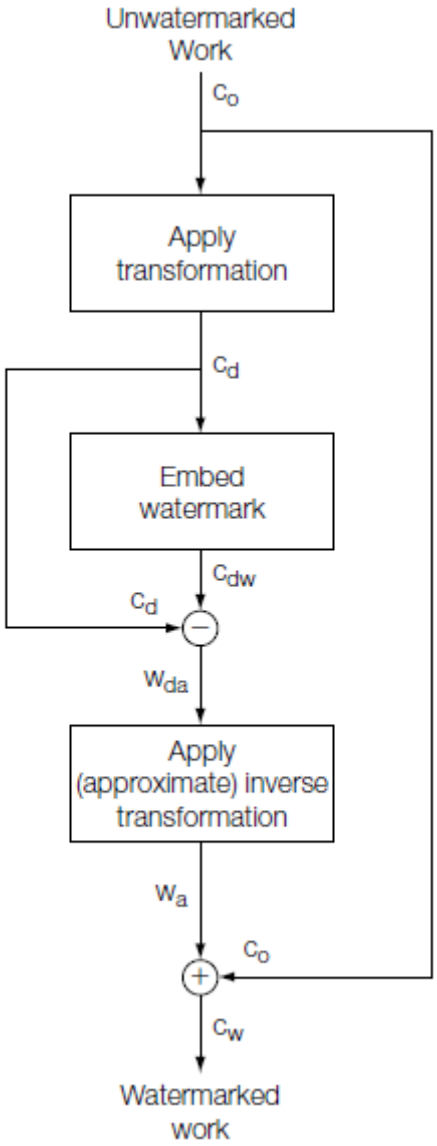
- Ҳақиқий контентга кутилиши мумкин бўлган ўзгаришни амалга ошириш (NTSC ёки PAL ҳолатига ўтказиш);
- Ўзгартирилган контентга белгини қўйиш. Бу ҳолда ембеддер контент ўзгартирилганлигини билмайди. У белгини ўзгармаган контентга қўйган каби буни амалга оширади.
- Белги мавжуд ўзгартирилган контент устида инверт ўзгартириш амалга оширилади.

Ушбу усул инвертлаш тўғри амалга оширилмаган ҳолда аниқлилик хусусиятини камайишига олиб келади. Шунинг учун юқоридаги кетма-кетликнинг охирги босқичида баъзи ўзрартиришларни киритиш талаб этилади. Бошқа сўз билан айтилганда жараён бироз мураккаблаштирилади:

- Ҳақиқий контентдан нусха олинади ва унинг устида кутилган ўзгариш амалга оширилади ва c_d қиймат олинади;

- Ўзгартирилган контентга watermarking белгиси қўйилади ва c_{dw} ҳосил қилинади;
- c_d га қўшили керак бўлган $w_{da} = c_{dw} - c_d$ қиймат топилади;
- Ҳақиқий контентга қўйилиши керак бўлган w_a белгини топиш учун w_{da} катталикни инвертланади;
- Ниҳоят, олинган w_a белги c_0 контентга бириктирилиб, c_w қиймат олинади.

Агар c_w контентга кутилган ўзгартиришлар амалга оширилганда, детектор томонидан c_{dw} белгига тенг бўлган белги аниқланади.



8.3 – расм. Белгини бириктириш жараёни

1.2. Бардошли watermarking тизимларига таъсирлар

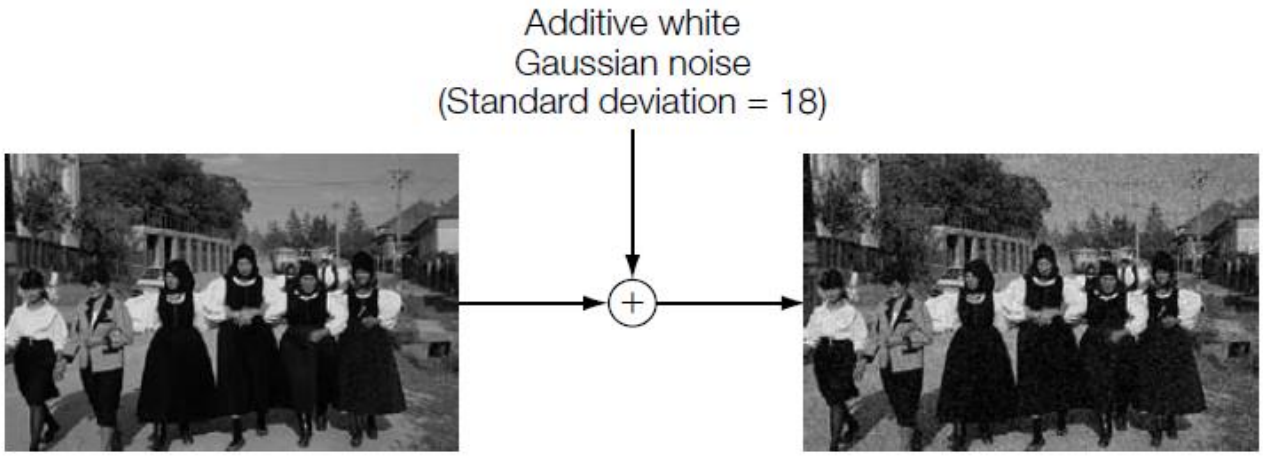
Бу бўлимда детекторлар ишига таъсир қилувчи тўрт турдаги ўзгартиришлар кўриб чиқилади. Булар қўшилган шовқин, амплитуданинг ўзгариши, чизиқли филтерлаш ва ёқотишли сиқиш. Бу ўзгаришларнинг

кўплари юқоридаги бўлимда айтилган усуллар асосида бартараф этилган.

Қўшилган шовқин. Контентда баъзи амаллар бажарилиши давомида унга тасодифий сигналлар қўшилиши мумкин. Яъни,

$$c_n = c + n$$

Бу ерда с контент ва n тасодифий шовқин. Бу шовқин контентга боғлиқ бўлмаган ҳолда турли тақсимотлар асосида қўшилади. Контентга боғлиқ бўлмаган ҳолда қўшилган тасодифий сигналга *қўшилган шовқин* деб аталади. Масалан, Гаусс усулида қўшилган шовқин, оқ рангли шовқин ва ҳак.



8.4 – расм. Шовқин қўшиш

Амплитуданинг ўзгариши. Назарий томондан тизимларни таҳлил қилинганда асосан қўшилган шовқин асосида ўзгиришга асосланган контентлар олинади. Сабаби, улар таҳлиллашга осон. Амалда эса бундан бошқа турдаги ўзгаришлар ҳам учрайди. Бу ўзгаришлар албатта контент маълумотнинг турига боғлиқ бўлади. Масалан, амплитуданинг ўзгариши:

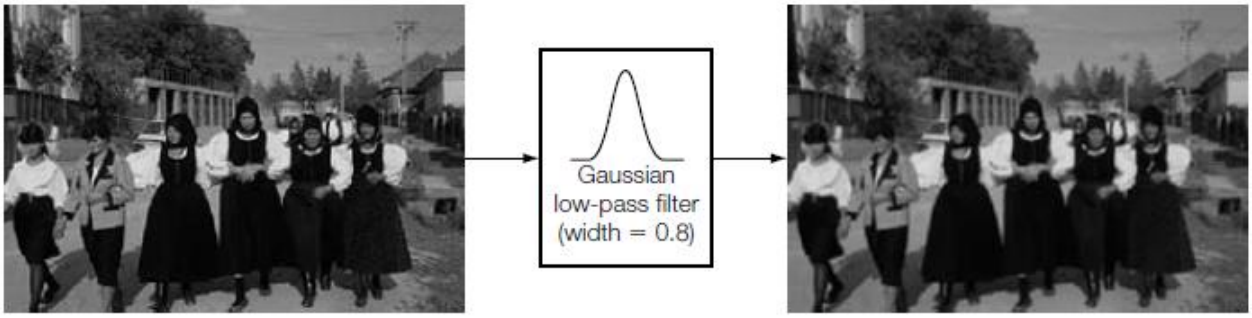
$$\mathrm{c}_v = vc;$$

Бу ерда с контент ва v ўзгартириш фактори. Бу катталик овоз маълумотлар учун овозни ўзгаришига олиб келса, видео маълумотлар учун эса ёритилганлик ва контрастни ўзгаришига олиб келади.

Чизиқли филтерлаш. Яна бир кенг тарқалган ўзгартириш усули бу чизиқли филтерлашдир. Бу катталик

$$c_n = c * f$$

каби ифодаланади. Бу ерда с контент, f филтер ва * боғланишни билдиради. Расм ва аудио маълумотлардаги кўплаб амаллар чизиқли филтерлаш орқали амалга оширилади. Расм маълумотларни қайта ишлаш учун кўплаб дастурий воситалар фойдаланилиб, уларда турли чизиқли филтерлаш амалларини бажариш мумкин.



8.5 – расм. Частотали филтерлаш

Ёқотишли сиқиш. Ўзгартирилишнинг бу турида ҳақиқий контент маълум усуллардан фойдаланган ҳолда сиқилади. Натижада сиқилган файл қайта очилганда ҳақиқий контентдан фарқ қиладиган ҳолда бўлади. Олинган фарқ сиқиш даражаси кўрсаткичига боғлик бўлади.

Назорат саволлари

1. Кенг поласали спектрум кодлаш.
2. Ўзгарувчанликка бардошли саналган коэффициент ўрнига қўйиш усули.
3. Белгиланган бардошлиликка эга коэффицентлар ўрнига қўйиш.
4. Детекторда ўзгаришларни инвертлаш.
5. Эмбеддерларда олдиндан инвертланган ўзгаришлар асосида.

Фойдаланилган адабиётлар

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, (2008). Digital Watermarking and Steganography, the Morgan Kaufmann Series in Multimedia Information and Systems, 2nd Ed.
2. Peter Wayner, (2008). Disappearing Cryptography, Second Edition - Information Hiding: Steganography and Watermarking, Morgan Kaufmann.
3. Bruce Schneier, (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C, second Edition, John Wiley & Sons.

9-маъруза

Watermark хавфсизлиги

Режа:

1. Хавфсизлик талаблари
2. Watermark хавфсизлиги ва криптография

Таянч иборалар: хавфсизлик талаблари, оммавий ва шахсий watermarking тизимлари, рухсатсиз белгини бириктириш, рухсатсиз белгини аниқлаш, рухсатсиз белгини олиб ташлаш.

Watermarking белгиси хавфсизлиги бу контентга қўйилган белгига бузғунчи томонидан турли ўзгартиришлар киритиш имкониятини йўқлиги билан белгиланади. Контентга қўйилган белгига бузғунчи томонидан турли бузулишлар амалга оширилиши мумкин ва бу бузулиш турлари watermarking тизимларига боғлиқ бўлади.

1.1. Хавфсизлик талаблари

Хавфсизлик талаблари watermarking иловалари турига боғлиқ ҳолда турлича бўлади. Масалан, баъзи watermarking белгилари барча турдаги бўлиши мумкин бўлган бузулишларга бардошли бўлса, баъзилари тизим хусусиятидан келиб чиқиб бўлиши мумкин бўлган бузулишларга бардошли қилиб ишлаб чиқарилади.

Watermarking амаллари чекланишлари. Ҳар бир watermarking тизимларида, баъзи фойдаланувчилар белги қўйиш ҳуқуқига, баъзилари белгини аниқлаш ҳуқуқига ёки ўчириб ташлаш ҳуқуқига ва қолганлари бу ҳуқуқлардан чекланган бўладилар. Хавфсиз Watermark бу чекланишлар қарши тура олишни талаб этади. Қуйидаги ценарийларни олайлик.

Ценарий 1. Алиса реклама берувчи бўлиб, ўз рекламаларига watermarking белгисини қўйиб, уларни 600 та радио тўлқинлари узра тарқатади. Кейин 600 та радио тўлқинлардан уларни детекторлаш орқали мониторинг қилади. Боб эса шу 600 та радио станциялардан бирида ишлайди. У Алисани рекламасини ўрнига, ўзини рекламасини юборишни хохлайди ва бунинг учун ҳақ ҳам тўлайди. Бунинг учун у Алиса қўйган белгини ўз рекламаларига бириктиради ва Алисанинг рекламаси ўрнига алмаштиради. Мониторинглаш жараёнида Алиса барча рекламаларини намойиш этилганлигини кўради. Аслида эса, Бобнинг ҳам рекламаси унинг рекламалари ўрнида намойиш этилади.

Ценарий 2. Алиса watermarking белгисини қўйувчи хизмат эгаси, номинал ҳақ олади. У Интернет тармоғи орқали тарқалувчи расмларга watermarking белгисини қўяди. Алиса шунингдек ҳамкорларга белги қўйилган расмларни Интернет тармоғида ги ҳолати бўйича қиммат статистик ҳисоботни тақдим этади. Ҳамкорлар бу ҳисобот асосида ўз расмларини қалбакилаштирилиш даражасини кузатиб борадилар. Боб Алиса томонидан белги қўйилган контентларни аниқлаш учун веб детектор тизимини яратади. Бу тизим орқали арзон статистик ҳисоботни тақдим этади. Сабаби, унда watermarking белгисини қўйиш талаб этилмайди. Боб таклиф этган хизмат арзон бўлганлиги учун барча ҳамкорлар Алисадан вос кечадилар.

Ценарий 3. Алиса кино студиосини эгаси ва у киноларини тарқатишдан олдин ўз киноларига кўчиришдан назоратлаш учун *copy-control* белгисини бириктиради. Алиса барча видео қурилмаларда кўчиришдан ҳимоялаш учун детектор мавжуд деб ҳисоблайди ва унинг маҳсулотларидан ҳеч ким фойдалана олмайди. Бобда видеода қўйилган мавжуд белгиларни ўчириш имкониятига эга қурилма мавжуд ва у Алисанинг видеоларини қалбакилаштира олади.

Кўриб ўтилган барча ценарийларда Боб Алиса томонидан қўйилган белгиларга рухсат этилмаган ҳолда таъсир этмоқда. 1 ценарийда *рухсат этилмаган қўйиш* амали бажарилмоқда. 2 ценарийда эса *рухсат этилмаган аниқлаш* амалини ва 3 ценарийда *рухсат этилмаган ўчириб ташлаш* амалини (ҳужумини) бажариш орқали Алиса томонидан қўйилган белгиларга таъсир этилмоқда. Ушбу уч турдаги ҳужумни амалга оширишда турли технологиялардан фойдаланилади.

Ҳар бир ҳужум турида ҳимояланишнинг муҳимлиги илова турига боғлиқ бўлади. Кимга қандан амалларни бажаришга рухсат берилганлигини аниқлаш, хавфсизлик талабларини таҳлил этиш фойдалидир. Берилган илова учун рухсатларни турли сондаги гуруҳларга ажратиш мумкин. Бу орқали ҳар бир гуруҳ учун қилиниши керак бўлган ва керак бўлмаган ишларни аниқлаш мумкин.

Қуйидаги жадвалда юқоридаги учта ценарий учун турли гуруҳларга берилган рухсатлар келтирилган. Бу келтирилган натижалар тизим ҳамма вақт шу ҳолатда ишлайди деганини исботламайди. Турли ўзгаришлар натижасида улар ўзгариши мумкин.

	Қўйиш	**Аниқлаш**	**Ўчириш**
ОАВ			

Реклама берувчи	Бор	Бор	-
Телевидения	Йўқ	Йўқ	-
Аҳоли	Йўқ	Йўқ	-
Веб ҳисобот			
Баҳолаш хизмати	Бор	Бор	-
Ҳисобот ҳизмати	-	Бор	-
Аҳоли	Йўқ	Йўқ	Йўқ
Кўчиришдан назоратлаш			
Контент провайдер	Бор	Бор	-
Аҳоли	-	Бор	Йўқ
Шахсий watermarking			
Ишончли шахс	Бор	Бор	-
Аҳоли	Йўқ	Йўқ	Йўқ
Оммавий watermarking			
Ишончли шахс	Бор	Бор	-
Аҳоли	Йўқ	Бор	Йўқ

Оммавий ва шахсий watermarking тизимлари. Юқоридаги жадвалда иккита махсус рухсатлар комбинацияси берилган. Бу рухсатлар иккита гуруҳга, ишончли саналган ҳодимлар учун ва бузғунчи бўлган фойдаланувчилар учундир. Биринчи рухсатлар комбинацияси *шахсий watermarking* тизимларига тегишли бўлиб, бунда аҳоли учун рухсатлар чекланган. Иккинчи рухсатлар тўплами *оммавий watermarking* тизимларига тегишли бўлиб, аҳоли учун фақат белгини аниқлаш имкони мавжуд. Қолган ҳолларда рухсатлар чекланган. Бу ҳолдаги шахсий ва оммавий watermarking тизимларига мос бўлган рухсатлар тўплами яратилаётган иловалар учун хавфсизлик талаблари деб аталади.

Таҳдид турлари. Юқоридаги жадвалда турли watermarking тизимларида уч турдаги рухсат тури ва уларни турли иловаларда турлича бўлиши келтирилган. Баъзида бу берилган рухсатлар бузулиш ҳоллари бўлиши мумкин. Жадвалда рухсатлар уч турдиги амаллар учун келтирилган. Watermarking тизимларида ҳам таҳдидлар айнан шу учта амални бузишга қаратилар экан.

Рухсатсиз белгини бириктириш. Кўплаб рухсатсиз белгини бириктириш усулида ихтиёрий олинган контентга ҳақиқий хабар белгиси қўйилади. Бу ҳол одатда хабарни бириктириш жараёни технологиясини ўрганиш натижасида келиб чиқади.

Рухсатсиз белгини аниқлаш. Бу турдаги таҳдидда белгини аниқлаш

рухсатига эга бўлмаган фойдаланувчи томонидан белгини аниқлаш амалга оширилади.

Қўйилган белгини рухсатсиз олиб ташлаш. Бу таҳдид натижасида контентдан белги рухсатсиз олиб ташланади ва белги қўйилмаган ҳолда келтирилади.

Тизимга таҳдид. Баъзи ҳолларда таҳдид белги қўйилган контентга қарши эмас, балки тизимга қарши амалга оширилади. Бунда тизимдаги баъзи бир заифликларга асослнади. Масалан, кўчиришни назоратлаш тизимларида ҳар бир қурилмаларда махсус микрочиплар бўлиб, улар белгини аниқлаш учун фойдаланилади. Ушбу микрочипни олиб ташлаш орқали, қурилмада ноқонуний тарзда нусхалаш имкониятини ҳосил қилиш мумкин. Бу Watermarking тизимига қилинган таҳдидга мисол бўла олади.

Таҳдидчининг имкониятлари. Таҳдидчи турли имкониятларга эга бўлиши мумкин. Масалан, қандайдир тизим учун таҳдидчи фақат белги қўйилган контент ҳақида маълумотга эга бўлса, бошқа бир тизимда умуман маълумотга эга бўлмаслиги мумкин. Қуйида бузғунчи имкониятлари ва оқибатлари келтириб ўтилган:

Бузғунчи ҳеч нимани билмаган ҳол. Бу ҳолда таҳдидчи тизим қурилмалари ва алгоритми ҳақида ҳеч қандай маълумотга эга бўлмайди. Бу ҳолда таҳдидчи барча watermarking тизимларида бўлиши мумкин бўлган ҳоллар ва алгоритмларни ўрганишдан бошлайди. Масалан, таҳдидчи контентни белги қўйилган деб ҳисоблайди ва ундан белги олиб ташлашга ҳаракат қилса, бунинг учун умумий усуллар саналган, маскалаш, турли геометрик, вақтинчалик ўзгаришларни, турли филтерлаш усулларини қўллаб кўришга ҳаракат қилади. Умумий ҳолда олинадиган хусусиятлар Stirmark тизимидан олиниши мумкин.

Таҳдидчига биттадан ортиқ белги қўйилган контентлар мавжуд бўлган ҳол. Баъзи ҳолларда таҳдидчига бир нечта белги қўйилган контентлар мавжуд бўлади. Бу ҳолда у алгоритмни билмаган ҳолда ҳам белгини олиб ташлашга ҳаракат қилади. Бу ҳолда кенг фойдаланиладиган усул бу *коллизия таҳдидидир.*

Коллизия таҳдидининг иккита йўналиши мавжуд. Биринчисида таҳдидчи бир хил белги бириктирилган бир нечта контент олади ва уларни ўрганиш орқали алгоритмни аниқлашга ҳаракат қилади. Масалан, содда ҳолда таҳдидчи барча бир хил белги мавжуд контентларнинг ўртача қийматини ҳисоблайди. Агар бир хил белги яшаринган бўлса у ҳолда олинган қиймат контентлар қийматига яқин бўлади. Олинган ўртача қийматни контентдан олиб ташлаш орқали белгини ўчириш имконияти туғилади. Бу усул айниқса аудио watermarking тизимларида катта самара

беради.

Коллизия таҳдидининг иккинчи усулида бир контент нусхаларида турлича белгилар қўйилган бўлиб, таҳдидчи барча белги қўйилган нусхалар орқали ҳақиқий контентни олишга ҳаракат қилади. Масалан, баъзи контент белгилари олиб ташланиши мумкин ва ҳак.

Таҳдидчи алгоритмни билган ҳол. Одатда қатий хавфсизлик талаб этилган тизимда таҳдидчи тизим алгоритми ҳақида тўлиқ маълумотга эга бўлмайди. Баъзи ҳолларда алгоритмни тўлик хавфсиз сақлашни имкони йўқ. Бундан ташқари алгоритмни махфий сақлаш натижасида, унинг хавфсизлигини тўлиқ таъминлаб бўлмайди.

Шунинг учун амалда алгоритм махфий тутилмайди. Фақат унга тегишли бўлган махфий калитлар сир тутилади. Таҳдидчи алгоритм ҳақида тўлиқ маълумотга эга бўлиш орқали бириктирилган маълумотни аниқлаши мумкин. Алгоритм маълум бўлган ҳолда ҳам таҳдидчи томонидан буза олмаслилик алгоритмнинг бардошлилиги юқори эканлигини англатади.

Таҳдидчига детектор маълум бўлган ҳол. Юқорида таҳдидчига алгоритм маълум бўлган ҳол ёки баъзи қисм маълумотлар маълум бўлган ҳоллар кўриб ўтилди. Бундан ташқари таҳдидчи детектор қурилмасига эга бўлган ҳол ҳам мавжуд бўлиб, би қарашда бу таҳдидчи фақат белгини аниқлаш имкониятига эга бўлади деган хулосани беради.

Таҳдидчи детектор қурилмасига эгалик қилган ҳолда, контентда маълум ўзгаришларни амалга ошириб, контентдан аниқланиш регионини аниқлаши ва бунинг натижасида алгоритмни аниқлаш имконига эга бўлиши мумкин.

1.2. Watermark хавфсизлиги ва криптография

Бу бўлимда криптография ва watermarking тизимлари орасида ўхшашлик ва алоқадорлик ҳақида тўхталиб ўтилади.

Watermarking ва криптографиянинг аналоглиги. Watermarking ва криптография тизимлари бир-бирига ўхшаш бўлиб, бу ўхшашликни қуйидаги тенгликлар орқали ҳам кўриш мумкин.

Криптографияда маълумотлар шифрлаш ва дешифрлаш (симметрик шифрлаш алгоритмлари учун):

Шифрлаш: $c = E_K(m)$; Бу ерда m – очиқ матн, c – шифр матн ва E_K шифрлаш функцияси.

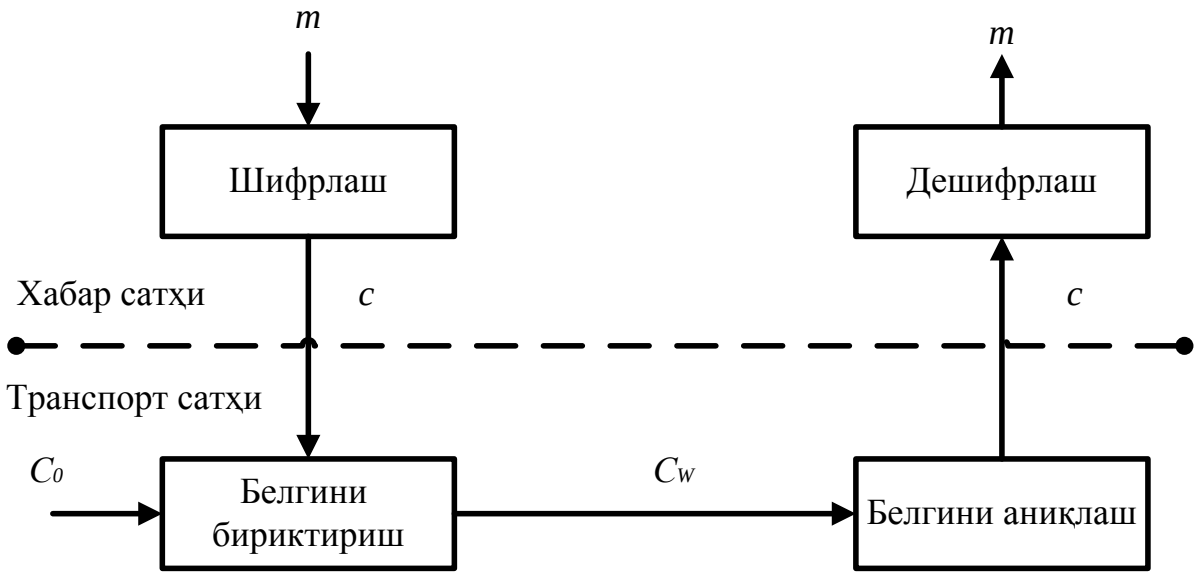
Дешифрлаш: $m = D_K(c)$; Бу ерда m – очиқ матн, c – шифр матн ва D_K дешифрлаш функцияси.

Watermarking тизимлари ҳам шунга ўхшаш бўлиб, белгиларни бириктириш ва ажратиб олиш босқичларидан иборат:

Белгиларни бириктириш: $c_w = \varepsilon_K\ c_0, m$, Бу ерда: ε_K – бириктириш функцияси, c_0 – ҳақиқий контент ва m – белги.

Белгиларни аниқлаш : $m = D_K\ c_w$, Бу ерда: $D_K -$ белгиларни аниқлаш функцияси.

Рухсат этилмаган аниқлашдан ҳимоялаш. Watermarking тизимларида криптография алгоритмларидан фойдаланиш орқали watermarking тизимларида мавжуд кўплаб таҳдидларни бартараф этиш мумкин. Қуйидаги расмда рухсат этилмаган аниқлаш таҳдидини криптографий усуллардан фойдаланиш орқали бартараф этиш кўрсатилган:



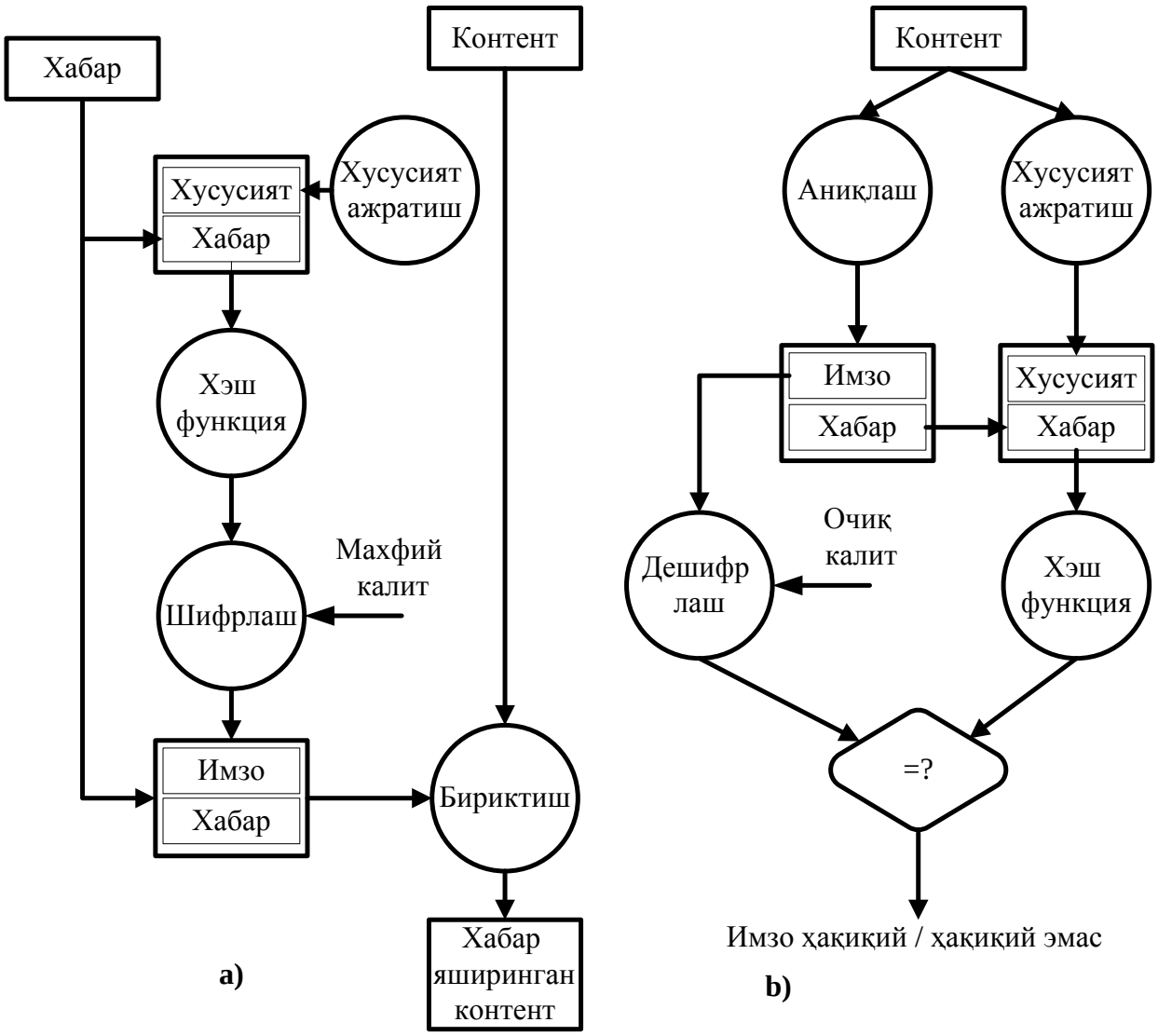
9.1 – расм. Рухсат этилмаган ўқишдан ҳимоялаш

Белгиларни рухсат этилмаган қўйишдан ҳимоялаш. Бу усулда ҳам криптографик ҳимоя усулларидан фойдаланилади. Криптографияда аутентификациялаш жараёнини амалга ошириш учун очиқ калитли шифрлаш ва электрон рақамли имзо алгоритмларидан кенг фойдаланилади.

Очиқ калитли шифрлаш алгоритмларида иккита калитдан фойдаланилади. Биринчиси маълумотни шифрлашда ва иккинчиси дешифрлашда фойдаланилади. Маълумотни шифрлаш калитлари барчага маълум бўлади. Дешифрлаш калити эса фақат калит эгасига маълум бўлади.

Электрон рақамли имзо алгоритмлари юборилган хабарни айнан бир фойдаланувчига тегишлигини англатади. Бу тизимлар ҳам иккита калитдан фойдаланади. Биринчи калит имзо чекиш учун (фақат битта фойдаланувчига тегишли бўлади), иккинчи калит эса имзони текшириш учун фойдаланилади (барчага маълум бўлади).

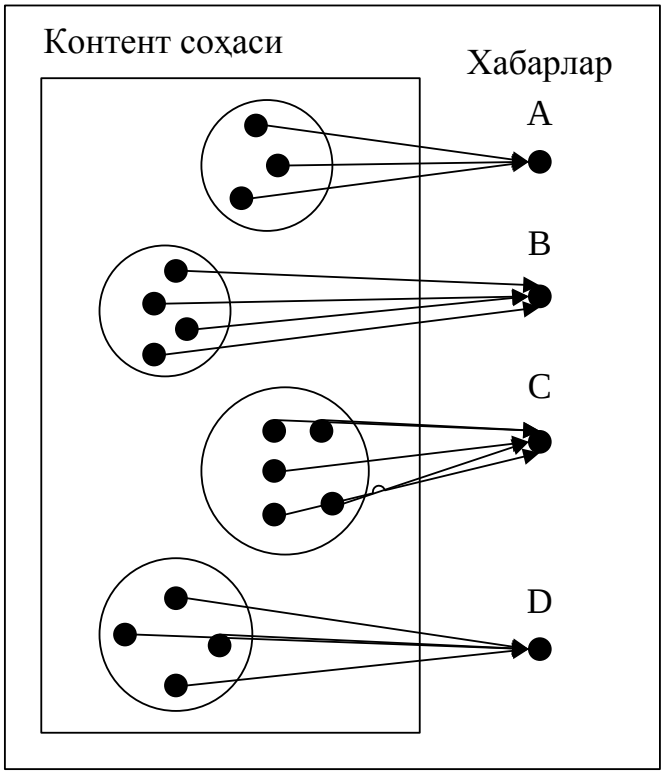
Қуйида электрон рақамли имзодан фойдаланган ҳолда белгиларни рухсат этилмаган қўйишдан ҳимоялаш усули келтирилган.



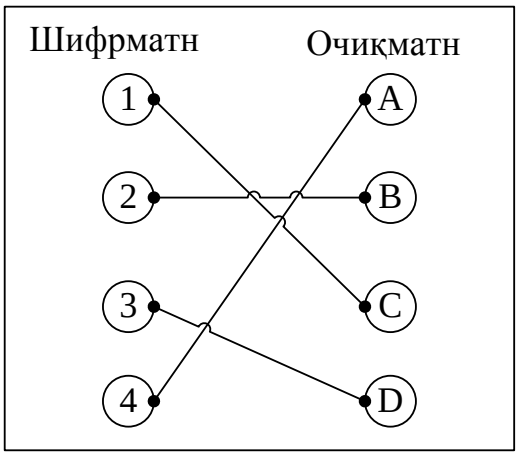
9.2 – расм. a) белгини бириктириш b) белгини аниқлаб олиш

Рухсат этилмаган олиб ташлашдан ҳимоялаш. Криптографик ҳимоя усулларидан фойдаланган ҳолда рухсат этилмаган қўйиш ва аниқлашдан соддалик билан фойдаланиш мумкин. Аммо, рухсат этилмаган олиб ташлаш криптографик муаммо саналмайди.

Рухсат этилмаган олиб ташлаш таҳдидига қарши *кенг полосаларда* модуляциялаш усулидан фойдаланилади. Бу усулда модуляцияланганда маълумотлар турли частоталарда ифодаланади. Қуйида кенг полосаларда модуляциялаш ва криптографик ҳимоя усули орасидаги боғланиш келтирилган.



Белгини бириктириш



Шифрлаш

9.3 – расм. Кенг паласаларда модуляциялаш ва шифрлаш усуллари

Назорат саволлари

1. Watermarking амаллари чекланишлари.
2. Оммавий ва шахсий watermarking тизимлари.
3. Таҳдид турлари.
4. Watermarking ва криптографиянинг аналоглиги.

Фойдаланилган адабиётлар

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, (2008). Digital Watermarking and Steganography, the Morgan Kaufmann Series in Multimedia Information and Systems, 2nd Ed.
2. Peter Wayner, (2008). Disappearing Cryptography, Second Edition - Information Hiding: Steganography and Watermarking, Morgan Kaufmann.
3. Bruce Schneier, (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C, second Edition, John Wiley & Sons.

10-маъруза

Контент аутентификацияси

Режа:

1. Аниқ аутентификациялаш.
2. Махсус аутентификациялаш.
3. Аниқланишлар.
4. Қайтариш.

Таянч иборалар: аутентификация, аниқланишлар, қайтариш, нозик watermarking, имзоларни бириктириш, олиб ташланувчан watermarking белгилар.

Бу маърузада watermark белгисини қўйилган контент бутунлигини текширишда фойдаланилиши кўриб чиқилади.

1.1. Аниқ аутентификациялаш

Аксарият аутентификациялаш тизимининг вазифаси бу контентнинг юборувчи ва қабул қилувчи томонлар орасида алмашинувида ўзгаришларга учрамаганлигини аниқлашдир. Ҳаттоки контентнинг бир битининг алмашиниши контентни аутентификация жараёнидан ўтмаганлигини англатади.

Аниқ аутентификациялаш watermarkingдан фойдаланишнинг иккита ёндошуви мавжуд. Биринчиси ҳолда watermarking белгиси шундай ҳосил қилинадики, белги қўйилган контеннинг ўзгариши белгини аниқланмаслигини таъминлайди. Иккинчи ёндошувда криптографик рақамли имзолардан фойдаланиш орқали, контент ўзгарган ҳолда имзони тегишли эмаслиги аниқланади.

Нозик watermarking белгилар. Нозик watermarking белгилари шундай белгиларки, контентнинг кичик ўзгариши бу белгиларни аниқланмаслигини таъминлайди. Шу вақтгача ўтилган мавзуларга тескари бўлган, бу хусусиятлар контентга бўлган таъсирларни муҳим эканлигини англатади. Нозик ўрнатилган белгилар аниқланса, демак контентга ўзгариш амалга оширилмаган. Акс ҳолда эса, контентга қандайдир ўзгариш амалга оширилган.

Энг кенг тарқалган нозик watermarking белгиларига LSB усулида қўйилган белгиларни олиш мумкин. Сабаби, бу усулда контентнинг энг кичик бити ўрнига маълумотнинг муҳимлиги катта бўлган бити яширинилади. Энг кичик бит эса ташқи таъсирларга жуда ҳам сезгир бўлади.

Имзоларни бириктириш. Имзолардан қандай тарзда фойдаланиш

криптографик иловалар учун тушунарли. Имзолардан watermarking тизимларида контент аутентификацияси учун фойдалаланиш мумкин. Криптографияда қўйилган имзо маълумотга сарлавҳа каби бириктирилса, watermarking тизимларида эса бу контент бўйлаб текис тақсимланади. Сарлавҳа каби қўйилганда уни осонлик билан олиб ташлаш имконияти мавжуд бўлади.

Қўйилувчи имзолар нозик watermarking белгилари шаклида ёки бардошли белгилар шаклида ифодаланади. Бардошли белгилар шаклида ифодаланганда контент устида ўзгаришларни амалга оширган тақдирдаҳам қўйилган белги ўзгармайди. Бунинг натижасида контент хусусиятидан ҳисобланган имзо ва аниқланган имзо бир – бирига тенглиги контентнинг ўзгармаганлигини, бир – бирига тенг бўлмаган ҳолда эса уни ўзгарганлигини билдиради. Нозик белгилардан фойдаланилган тақдирда эса бардошли белгилардан фойдаланилганга қараганда соддароқ бўлади. Конентга қўйилган нозик белги кичкина ўзгаришга таъсирли саналиб, детекторланганда бу белги аниқланмаса контентга ўзгаришлар амалга оширилган. Акс ҳолда контентга ўзгаришлар амалга оширилмаган.

Олиб ташланувчан watermarking белгилар. Баъзида контентга бириктирилган энг кичик ҳажмдаги имзо ҳам, контентга таъсир қилиши мумкин. Масалан, тиббиётга алоқадор иловаларда контентга бириктирилган имзо кам бўлса ҳам, контент ўзгаришига таъсир қилади. Бу эса шифокорни қарор қабул қилишига акс таъсир қилиши мумкин. Шу сабабли олиб ташланувчан watermarking белгиларни ишлаб чиқишни таълаб этади (белги қўйилган контентдан белгини олиб ташлаш ва ҳақиқий контентдан нусха олиш учун).

Қуйида олиб ташланувчан watermarking белгиларини яратишнинг асосий қадамлари келтириб ўтилган:

- Ҳақиқий контентнинг бутун юзаси бўйлаб имзо ҳисобланади. Ҳисобланган имзо контентга олиб ташланувчанлик хусусияти билан бириктирилади;
- Қабул қилувчи контентдан имзони ажратиб олади ва уни қайд этиб қўяди;
- Қабул қилувчи контентдан имзони олиб ташлайди. Бу ҳолатда олинган контент ҳақиқий контент билан бир – хил бўлиши керак;
- Буни текшириш учун қабул қилувчи белги олиб ташланган контентнинг *хэш қийматини* ҳисоблайди. Қайд қилинган имзони декодлаб олинган хэш қиймат билан контентнинг хэш қиймати бир – бирига мос келган тақдирда контент ўзгиришга учрамаган. Акс ҳолда контент ўзгаришга учраган;

Амалда олиб ташлунувчан белгиларни бириктириш жуда муаммоли саналиб, буни амалга оширишда қуйидаги учта шарт бажарилиши керак:

- Белгини бириктиришни 100 % самарадорлик билан амалга ошириш;
- Контентни қайта тиклаганда (контентдан белгини ажратганда) ҳақиқий ҳолатдагиси билан бир – хил бўлиши;
- Жуда кам миқдорда ёлғондан тасдиқлаш кўрсаткичини мавжуд бўлиши талаб этилади.

1.2. Махсус аутентификациялаш

Аниқ аутентификациялаш усули жуда кўп иловаларда фойдаланилади. Масалан, бу усулда фойдаланилганда контентдаги бир-иккита битларни ўзгариши натижани тамомила бошқа кўринишга олиб келади. Бошқа сўз билан айтилганда бу усул ўзгаришларга жуда ҳам тасирчан. Шунга қарамасдан, контент устида баъзи ўзгаришларни амалга оширганда контентнинг кўринишига жиддий таъсир этмайди (10.1 - расм).

Ҳақиқий контент JPEG форматда (95 % аниқлик билан сиқилишдаги)

10.1 – расм. Махсус аутентификациялаш

Олинган расмлар бир – бирига жуда ўхшасада, улар аниқ аутентификациядан ўта олмайди. Бу эса *махсус аутентификациялаш* усулини яратишга сабаб бўлади. Бу усулда контент устида муҳим ўзгариш содир бўлган тақдирдагина аутентификациядан ўта олмаслик мумкин бўлади.

Ноқонуний ва қонуний ўзгаришлар. Махсус аутентификациялаш усуллари контентга қуйидаги, йўқотилишли чиқиш, филтерлаш, таҳрирлаш ва ҳак. ўзгаришлар амалга оширилганда талаб этилади. Бу ўзгаришлар ўз навбатида икки турга: *қонуний ва ноқонуний ўзгаришларга* ажратилади. Контент қонуний ўзгаришга учраганда тизим контентни аутентификациялашдан муофаққиятли ўтади ёки ноқонуний ўзгаришларга учраган контент аутентификациялашдан ўта олмайди.

Одатда контентга қонуний ва ноқонуний ўзгаришлар амалга оширилганда яққол кўринишидан фарқланади. Масалан юқоридаги 10.1 –

расмда амалга оширилган ўзгаришни қонунуй деб олиш мумкин. Қуйида келтирилган ўзгаришни эса ноқонуний ўзгаришга киритиш мумкин (10.2 - расм).

Ҳақиқий контент

Таҳрирланган контент

10.2 – расм. Ноқонуний ўзгаришлар

Юқоридаги икки расмдан қонуний ва ноқонуний ўзгаришларни яққол ажратиш мумкин. Амма, 10.3 – расмда келтирилган ҳол учунчи ?

Ҳақиқий контент

JPEG форматда (20 % аниқлик билан сиқилишдаги)

10.3 – расм. Қонуний ўзгаришлар

Жавоб эса контентга боғлиқ ҳолда аниқланади. Ўзгаришларни қонуний ва қонуний бўлмаган турларга ажратиш етарлича катта муаммо саналади.

Ярим-нозик watermarking белгилари. Бу турдаги белгиларга қонуний ўзгаришлар таъсир этмайди, ноқонуний ўзгаришлар эса тасир этади. Бу турдаги белгиларни яратиш махсус аутентификациялаш усулларини ишлаб чиқишда ёрдам беради. Ярим-нозик watermarking белгиларини ишлаб чиқишда, белгини қонуний ўзгаришларга бардошлилиги таъминланса, шунинг ўзи етарли саналади.

Назоратчи ёки чақимчи watermarking белгилари. Юқори ярим-нозик белгилардан фойдаланишдан мақсад, қонуний ва ноқонуний орасидаги

фарқни аниқлашдан иборатлиги айтиб ўтилди. Шунга қарамасдан, баъзи watermarking тизимларида қонуний ва ноқонуний ўзгаришлар орасидаги фарқ вақт ўтиши билан, жой ўзгариши билан ўзгариб туради. Бу ҳолда кўпроқ контент ўзгаришга учрадими деган саволдан кўра, контент қайдай ўзгаришга учради деган савол муҳимроқ саналади. Бу саволни жавобини аниқлашда *Назоратчи ёки чақимчи watermarking белгиларидан* фойдаланилади.

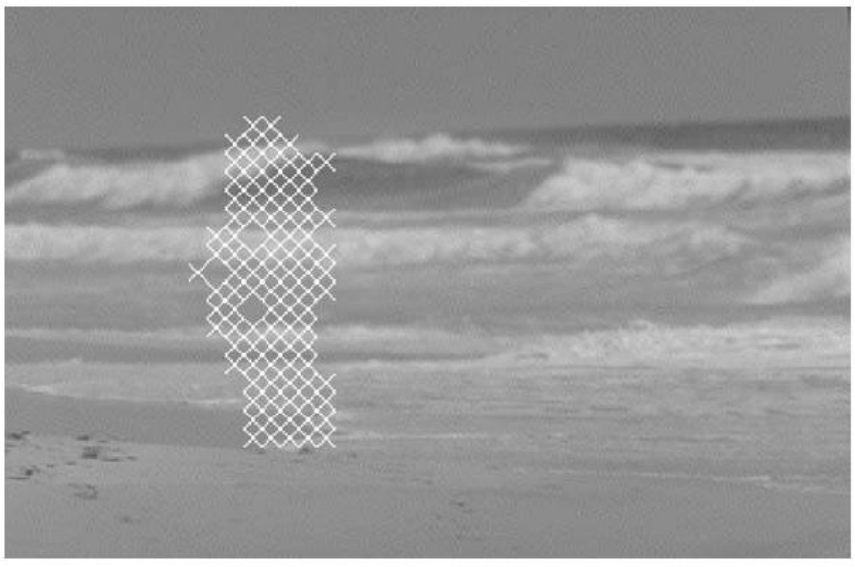
1.3. Аниқланишлар

Кўплаб аутентификациялаш методлари бириктирилган белгини қачон ва қайерга қўйилганинини аниқлашга асосланади. Контентнинг қолган қисми эса ўзгармасдан қолади. Бу қобилят – *аниқланиш* деб айтилади.

Белгиларни қайерда ва қачон яширинганлигини билиш орқали белгини ўзгарган ёки ўзгармаганлигини аниқлаш, аутентификациялашни амалга ошириш мумкин.

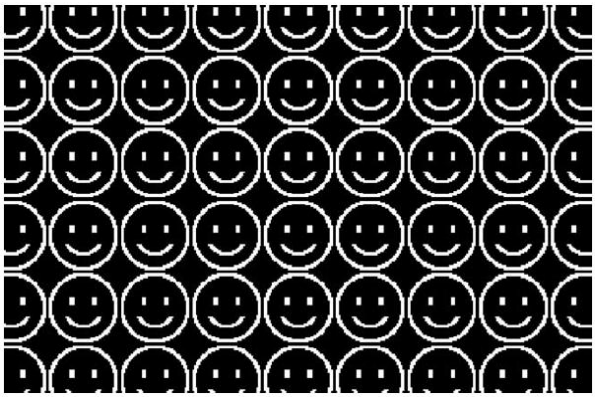
Аниқлашда қуйидаги икки ёндошув кенг фойдаланилади:

Блошлашга асосланган контент аутентификацияси. Бу усулда асосланган аутентификациялашда контент бир нечта вақт ёки майдон хусусияти бўйича блокларга бўланади. Белги ҳам ҳар бир блок учун алоҳида-алоҳида қўйилади. Аутентификациялаш ҳар бир блок устида амалга оширилади. Агар ўзгариш амалга оширилган тақдирда фақат ўзгарган блок аутентификациялашдан ўта олмайди.

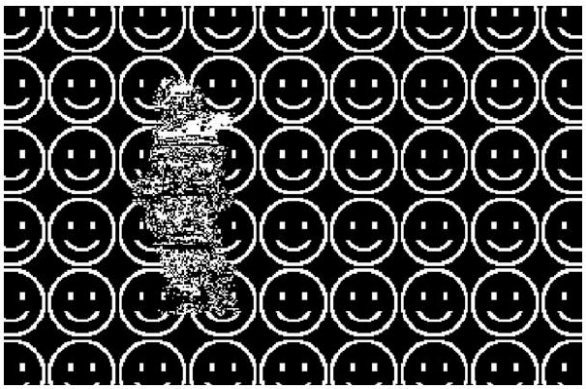


10.4 – расм. Блоклашга асосланган аутентификациялаш

Наъмунага асосланган аутентификациялаш усули. Бу усул блоклашга асосланган усулнинг бир хусусий ҳоли бўлиб, бунга кўра контент кўплаб кичкина блокларга эмас, балки ягона блокларга ажратилади.



Наъмуналарга ажратиш



Наъмунага асосланган аутентификациялаш

10.5 – расм. Наъмунага асосланган аутентификация

1.4. Қайтариш

Ўтилган барча маърузалардан келиб чиқиб, контент ўзгарган тақдирда ҳам белгини аниқлаш имкони мавжудлигини айтиш мумкин. Бу эса ўз навбатида ўзгарган контентни қайтариш имконини мавжудлигини англатади.

Икки хил усулда қайтариш имкони мавжуд бўлиб, улар: *аниқ қайтариш* ва *тақрибий қайтариш.* Номига боғлиқ ҳолда, аниқ қайтаришда ўзгарган контент ўзининг ҳолатида тўлиқ қайтарилади ва бу анча катта муаммодир.

Тақрибий қайтаришда эса хатолик билан қайтарилади. Бу усул амалда кенг фойдаланилади. Қуйида буларнинг ҳар бири билан алоҳида танишиб чиқилади.

Бириктирилган қолдиқ маълумот. Бу усул аниқ қайтариш усулига киради. Бу усулдаги қайтаришда хатоликларни аниқлаш ва тузатиш кодлари кенг фойдаланилади. Контентни ўзгариши хатоликларни тузатиш имконияти даражасида бўлса, у ҳолда ўзганган контент тўлиқ қайтарилади.

Хатоликларни тузатиш кодлари ЭРИ алгоритмларига ўхшасада, улардан вазифаси жихатидан кенгроқдир. ЭРИ алгоритмлари фақат ўзгаришни аниқласа, хатоликларни тузатиш кодлари эса уларни тузатади ҳам.

Ўзини ўзига бириктириш. Бу усул тақрибан қайтариш усулига киради. Кўплаб манбаларда, контент сиқилган кўринишини контентнинг ўзига бириктириш амалга оширилади. Бу усул *ўзини ўзига бириктириш* усули деб юритилади. Бунга мисол сифатида қуйидагини олиш мумкин. Ҳақиқий контент расм олиниб, ундан 50 % сиқилган JPEG форматдаги кўриниши олинади. Бу ҳолда ўртача бир пикселдан бир битига тенг бўлади. Олинган бир бит мос ҳақиқий контентга LSB усулида бириктирилади.

Кўркўрона қайтариш. Бу усул ҳам тақрибан қайтариш усулига киради.

Бу усулга асосан дастлаб контентнинг ўзгарган қисмлари аниқланади ва улар инвертлаш орқали дастлабки ҳолатга қайтарилади. Бу усул фақат ўзгаишлар инвертлаш хусусиятига эга бўлган тақдирдагина катта ютуқ беради.

Назорат саволлари

1. Аутентификация.
2. Аниқ ва махсус аутентификация.
3. Ўзгаришлар.
4. Қайтариш.

Фойдаланилган адабиётлар

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, (2008). Digital Watermarking and Steganography, the Morgan Kaufmann Series in Multimedia Information and Systems, 2nd Ed.
2. Peter Wayner, (2008). Disappearing Cryptography, Second Edition - Information Hiding: Steganography and Watermarking, Morgan Kaufmann.
3. Bruce Schneier, (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C, second Edition, John Wiley & Sons.

11-маъруза

Стеганография

Режа:

1. Стеганографик алоқа тизимлари.
2. Термин ва изоҳлар.

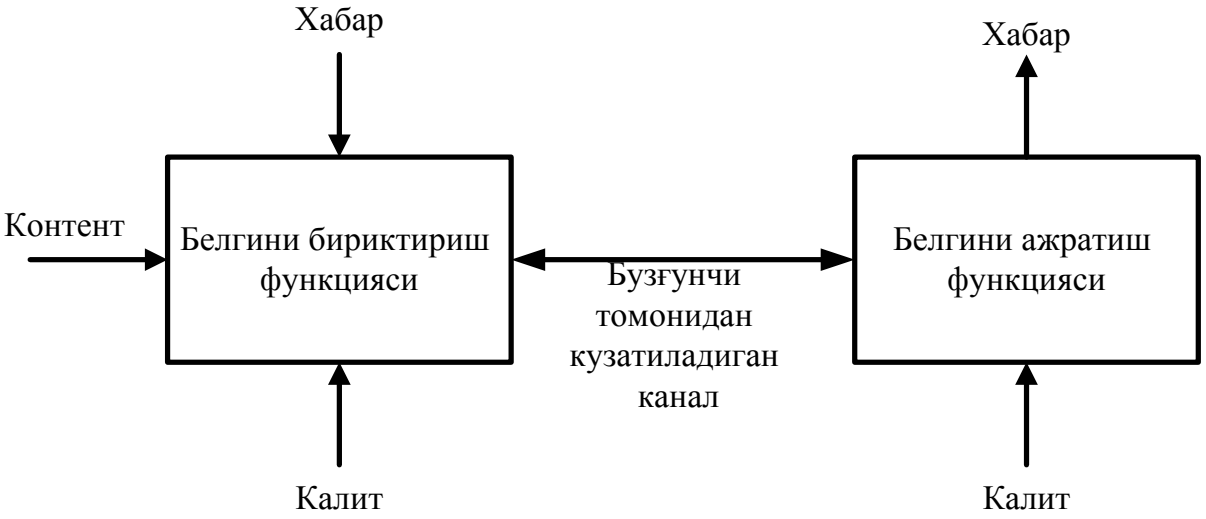
Таянч иборалар: Стеганорафия, алоқа тизимлари, маълумотларни яшириш, криптографик усуллар.

Стеганография маълумотларни яшириш усулларини ўрганиб, бунда яширинган маълумотни фақат юборувчи ва қабул қилувчи билиши мумкин. Стеганография тизимларига қўйиладиган асосий талаблардан бири бу – аниқлаб бўлмасликдир. Бошқа сўз билан айтганда бузғунчи контентда маълумот яширинганлигини билмаслиги шарт ва зарур.

Watermarking ва стеганография тизимлари маълумотларни яширувчи икки асосий кўриниш саналсада, уларнинг орасида муҳим фарқ мавжуд.

1.1. Стеганографик алоқа тизимлари

Стеганографиянинг дастлабки формал бўлмаган кўринишдаги схемаси, Симонс томонидан *маҳбуслар муаммоси* тарзида ифодаланган. Бунга асосан икки махбус бир-бири билан маълумот алмашаши керак. Аммо маълумот алмашинувини қамоқ бошлиғи назорат қилади. Бунда икки маҳбус шундан усул орқали маълумотни яшириши керакки натижада қамоқ бошлиғи яширинган маълумотни аниқлай олмасин. Ушбу схема қуйида келтирилган.



11.1 – расм. Стеганографик тизим

Маълумотни узатиш канали. Стеганографияда одатда алоқа физик

каналлар орқали амалга оширилади. Умумий ҳолда шовқин бўлишини ҳисобга олиб, бу тизимларда хатоликларни тузатиш кодларидан фойдаланилади. Ўртада бузғунчи борлигини ҳисобга олган ҳолда, уларни уз турга: актив, пассив ва зарарли турларга ажратиш мумкин.

Пассив турдаги бузғунчи ўртада узатилаётган маълумотни кузатиш имконига эга бўлади. Агар яширинган маълумот топилса унда алоқа узилади. Акс ҳолда алоқага тегинилмайди.

Актив турдаги бузғунчи ўртада узатилаётган маълумотни кузатибгина қолмай, яширинган маълумот топилмаган тақдирда контентга ўзратириш киритади ва яширинган маълумотни аниқлаб бўлмас ҳолатга келтиради ва қабул қилувчига юборади.

Зарарли турдаги бузғунчи ўртада туриб, ҳар икки томонга ёлғон маълумотларни узатади. Бу одатда очиқ калитли тизимлардан фойдаланилган ҳолда ўхшайди. Яъни, алдамчи маълумотларни юбориш орқали томонларни чалғитиш ва алдаш амалга оширилади.

Стегонографиянинг қурувчи блоклари. Стегонографик алгоритмларнинг қуришнинг асосий блоклари қуйидагилар:

- Яширувчи маълумотни, контентни танлаш;
- Қуйидагиларни ўз ичига олган бириктириш ва ажратиш алгоритмлари:
    - Белгиларни тайинлаш функцияси;
    - Бириктириш ўзгартиришлари;
    - Танлаш қоидалари.
- Стего калитларни бошқариш.

Стегонография тизимлари Watermarking тизимларига ўхшамаган ҳолда яширувчи маълумот, контент ҳақида маълумотни ўзида сақламайди. Натижада эса маълумотни ташувчи контентларни ихтиёрий танлаш имконияти вужудга келади.

Белгиларни яшириш, қўйиш функцияси қуйидаги учта асосий принсипга асосланади:

- Маълумотни яширувчи контент олдиндан мавжуд бўлиб, ембеддер контентни ўзгартирмайди. Бу эса стегонографияда маълумотни яшириш “қараш” орқали амалга оширилади.
- Маълумотни ташувчи контент махфий маълумот асосида яратилади ва контент ҳеч қандай ўзгартирилмайди. Бу принсип контентни синтезлаш деб ҳам аталади.
- Контент олдиндан аниқланган бўлади ва эмбеддер контентни ўзгартиради. Бу усул контентни ўзгартириш орқали стегонография усули деб ҳам аталади.

Қандай қилиб контентни ўзгартирмасдан маълумотни яшириш мумкин? Масалан, Алиса 10-битли маълумотни Бобга юбормоқчи. Бунинг учун Алиса 1 000 га яқин қўшиқни олади ва уларнинг ҳар бирига махфий калитини бириктириб, хэшлайди ва натижани юбормоқчи бўлган маълумоти билан солиштиради. Натижа тенг бўлса, у ҳолда шу қўшиқ танланади, акс ҳолда кейинги қўшиқ олинади ва ҳисоблаш амалга оширилади. Бу усулнинг мураккаблиги керакли бўлган контентни топиш даражаси билан аниқланади.

Синтезлаш усулига кўра, дастлаб махфий маълумот олиниб, кейин уни яширувчи контент танланади. Бунга мисол сифатида иккинчи жаҳон урушида фойдаланилган “Windswept” кодларини олиш мумкин. Бунга асосан, суҳбатлашиш учун керакли бўлган бирикмалар қатори маълум бир код билан белгиланган. Бу кодлар орқали эса бирикмани топиш имкони яратилади. Бу кодлар тўплами махсус китоб шаклида ишлаб чиқилган.

Контентни ўзгартиришга асосланган стегонографияда эса контентни маълумотга қараб ўзгартириш амалга оширилади. Ўзгартиришлар танлаш қоидаларига асосан танланади.

Контентга маълумотни яшириш калитлар асосида амалга оширилган. Бу калитлар турли мақсадларда фойдаланилган.

1.2. Термин ва изоҳлар

Ушбу бўлимда стегонографиянинг математик томондан талқини кўриб ўтилади. Фараз қилайлик, K_s стего калит калитлар тўплами K олинган. M юборилиши керак бўлдиган махфий маълумотлар. C эса яширувчи контент. Бу ҳолда эмбеддерлаш ва аниқлаш жараёнлари қуйидагича ифодаланади:

Эмбед: $CxKxM \to C$

Аниқ: $C \to M$

Хусусий ҳолда эса, ажратилган белги $c \in C, K_s \in K$ ва $m \in M$ бўлган ҳолда $Ext\ \ Emb\ \ c, K_s, m\ \ \ = m$ га стегоконтент эса $s = Emb\ \ c, K_s, m\ .$

Бу ерда Ext – белгини ажратиш функцияси, Emb – белгини бикиртириш функцияси.

Назорат саволлари

1. Маълумотларни яшириш.
2. Стегонографик ҳимоя.
3. Алоқа каналлари.
4. Криптографик ҳимоядан фойдаланиш.

Фойдаланилган адабиётлар

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, (2008). Digital Watermarking and Steganography, the Morgan Kaufmann Series in Multimedia Information and Systems, 2nd Ed.
2. Peter Wayner, (2008). Disappearing Cryptography, Second Edition - Information Hiding: Steganography and Watermarking, Morgan Kaufmann.
3. Bruce Schneier, (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C, second Edition, John Wiley & Sons.

12-маъруза

Стегонотаҳлил

Режа:

1. Стегонотаҳлил сенарийси.
2. Расм маълумотлар стегонографияси.

Таянч иборалар: таҳлил, стегонотаҳлил, аниқлаш, кўркўрона стегонотаҳлил, мақсадли стегонотаҳлил.

1.1. Стегонотаҳлил сенарийси

Стегонотаҳлил соҳаси стегонография соҳасига қарама-қарши ҳисобланиб, унда стегонография усулларининг бардошлиги таҳлил қилинади.

Стегонотаҳлил сенарийси умумий ҳолда иккита қонуний фойдаланувчи орасида узатилган яширинилган махфий маълумотни аниқлашдан иборатдир.

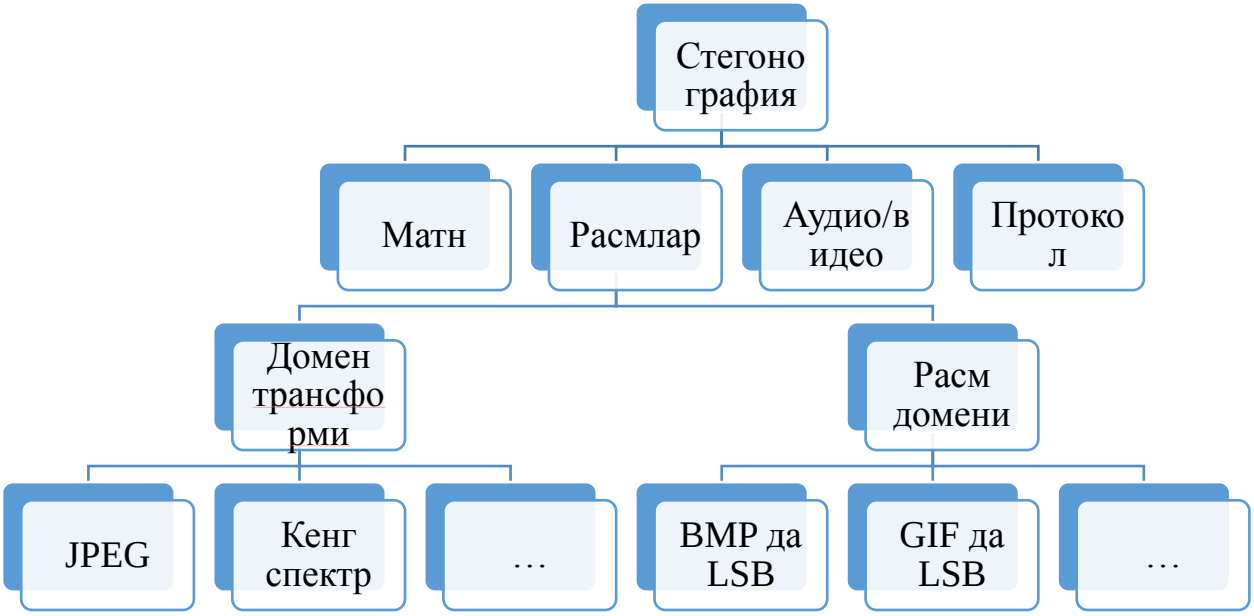
Аниқлаш. Аниқлаш жараёни контентга махфий белги яширинилганми ёки йўқлигини аниқлаш бўлиб, аниқлаш жараёни натижасида контентнинг шунчаки контентлиги ёки стегоконтентлиги (белги яширинилганлиги) аниқланади.

Стегонотаҳлилни олиб борувчи бузғунчи стегонотаҳлилчи деб юритилади ва унинг асосий вазифаси унга маълум бўлган ахборотларга асосланган ҳолда контентда белги мавжуд ёки мавжуд эмаслигини аниқлаш. Стегонотаҳлилчига гоҳида ҳеч қандай маълумот маълум бўлмаслиги, фақат махфий алоқадан фойдаланилишини билиш мумкин. Баъзида, стегонотаҳлилчига фойдаланувчилар томонидан фойдаланилган стегонографик алгоритм маълум бўлади. Биринчи ҳолатда стегонотаҳлилчи белгиларни топишда, умумий усуллардан фойдаланади ва бу кўринишдаги стегонотаҳлил усули *кўркорона стегонотаҳлил* усули деб аталади. Иккинчи ҳолатда эса, стегонотаҳлилчи аниқ бир алгоритмни таҳлил қилади ва бу кўринишдаги стегонотаҳлил усули *мақсадли стегонотаҳлил* усули деб аталади.

1.2. Расм маълумотлар стегонографияси

Расм маълумотлар стегонографияда енг кўп тарқалган маълумот ташувчи контент ҳисобланади. Расм маълумотларнинг рақамли ишлов беришда уларнинг форматларидан фойдаланилган ҳолда ёндошилади. Расм маълумотларнинг кўп турлари мавжуд бўлиб, улар тузилишлари билан бир – биридан фарқ қилади. Ҳозирда амалда .JPEG, .GIF, .BPM, .PNG, .TIFF каби кенг тарқалган турлари мавжуд. Ҳар бир расм форматлари турли хусусиятларга эга бўлганлиги сабабли, рақамли стегонографияда улардан

фойдаланишда унга этибор бериш керак. Масалан, .JPEG формати маълумотларни сиқишда йўқотиш усулларидан фойдаланилганлиги сабабли, ундан стегонографияда фойдаланилганда (расм устида ишлов бериб, уни яна расм сифатида .JPEG форматида сақлаганда) маълумотларни йўқолиш хавфи мавжуд бўлади.



12.1 – расм. Расм стегонографияси категориялари

Ёқотилишсиз сиқишга асосланган расм форматларига эса .GIF ва .BMP (8 - битли) форматларини олиш мумкин. Юқорида айтиб ўтилганидек, стегонографияда расм маълумотлардан фойдаланилганда уларни йўқотиш билан йўқотишсиз сиқиш ҳусусиятига этибор бериш керак.

LSB усули. Ушбу усулга кўра контентдаги пикселлар битларининг муҳим саналмаган ўринларидаги қийматини (LSB (least significant bit)) маълумот пикселлари битларига алмаштирилади. Ушбу усул қуйидагиларга асосланади:

- Расм маълум ўлчамга эга бўлганлиги сабабли (масалан, NxM), ихтиёрий (i,j) ўриндаги пикселини бинар ҳолда ифодалаш имконияти мавжуд;
- Бу ифодаланиш натижасида расм битларини муҳим саналган (most significant bit,MSB) ва муҳим саналмаган (least significant bit, LSB) битларга ажратиш имконияти туғилади.

Умумий ҳолда ушбу алгоритмнинг умумий моҳияти контентнинг муҳим бўлмаган позицияларини аниқлаш ва уни махфий маълумотнинг (watermarking белгиси) муҳим саналган позицияларидаги битлари билан алмаштиришга асосланган.

Ушбу алгоритмдан фойдаланишда контент ва махфий маълумот

сифатидаги расмлар *grayscale* моделида бўлиши мумкин. *grayscale* ранг моделида барча пикселлар 0-255 гача бўлган сонлар билан ифодаланади. Бу моделда берилган пикселдаги битларни муҳим ва муҳим бўлмаган битга ажратиш қуйидагича амалга оширилади: 201(11001001) пиксели учун улар қуйидагича (12.2 – расм).

	MSB						LSB
Бит индекси	8	7	6	5	4	3	2	1
Қиймати	1	1	0	0	1	0	0	1

12.2 – расм. Битларнинг жойлашувлари

Агар расм RGB ранг моделида бўлса, унда унинг ташкил этувчи ҳар бир қисми бир байтдан ифодаланади.

Ушбу усулга асосан расмнинг ҳар бир пикселининг 8 – битига (LSB) га яширинувчи маълумотнинг бир бити қўйилади. Агар расм RGB ранг моделида бўлса, унда бир пикселда уч бит маълумотни яшириш мумкин.

Масалан, RGB ранг моделидаги 3 – пиксел қуйидагича бўлса:

```
1 – пихел (00101101 00011100 11011100)
2 – пихел (10100110 11000100 00001100)
3 – пихел (11010010 10101101 01100011)
```

Яширинувчи маълумот 200 га (11001000 иккиликда) тенг. Маълумот яширинган пикселнинг кўриниши қуйидагига тенг бўлади:

```
1 – пихел (00101101 00011101 11011100)
2 – пихел (10100110 11000101 00001100)
3 – пихел (11010010 10101100 01100011)
```

Ўзгартирилган пикселлардан қайта расм ҳосил қилинганда (йўқотилишсиз сиқиш билан) инсон кўзи илғамас тарздаги ўзгириш содир бўлади. Бу усулдан фойдаланилганда BMP расм форматидан фойдаланиш тавсия этилади. Аммо, BMP форматидаги расмнинг ҳажми катта бўлиши талаб этилади. Шунинг учун ушбу усулнинг бошқа расм формати учун ишлаб чиқишга уринишлар ортмоқда.

LSB ва палитрага асосланган расмлар. Палитрага асосланган расмлар, масалан, GIF формати, Интернет тармоғида фойдаланиладиган яна бир кенг тарқалган расм тури ҳисобланади. GIF форматидаги расмларда ҳам бит узунлиги 8 га тенг ва шунинг учун максимал ранглар сони 256 та бўлади. Ушбу расм тури индексланган расм саналиб, расмларда мавжуд ранглар палитрада сақланади. Баъзида махсус жадваллар тарзида ифодаланадилар.

Ҳар бир пиксел ягона байт орқали ифодаланади ва пиксел маълумот индекс сифатида ранглар палитрасида сақланади. Бу ранглар палитраси одатда енг кенг тарқалган ранглардан енг кам тарқалган ранглар томонга қараб тартибланган бўлади.

GIF расмлар ҳам LSB стегонографиясида фойдаланилади ва катта этиборни талаб этади. GIF расмлардаги ушбу муаммо, пиксел LSB битининг биргина ўзгариши, палитрадаги индекслар ўзгариши натижасида бутин расмга таъсир этиши мумкин. Бунинг олдини олишнинг бир усули бу палитрадаги рангларни тартиблашдир. Яъни, палитрани шундай тартиблаш керакки, кетма – кет келган ранглар орасидаги фарқ жуда кичик бўлсин. Ушбу муаммони ҳал қилишнинг ишончи усули бу – *grayscale* расмлардан фойдаланишдир. Бунда маълумот яширинган расмларда жуда кичик ўзгаришлар содир бўлади ва натижада таҳдидчи ушбу ўзгаришни пайқай олмайди.

JPEG сиқиш. Расмни JPEG форматга сиқишдан олдин, RGB ранглар YUV кўринишида ўтказилади. Бунда Y ташкил этувчи ёруғлик миқдорини, U ва V рангларни ифодалайди. Тажрибилар шуни кўрсатадики, инсон кўзи ранглар ўзгариши фарқидан кўра, ёруғлик ўзгариши фарқини яхшироқ ажратади. Ушбу факт JPEG сиқишда фойдаланилган, яъни расм файлининг ўлчамини камайтириш учун ранглар маълумотлари камайтирилади. Ранглар ташкил этувчиси (U ва V) горизонтал ва вертикал йўналишни ифодалагин сабабли, расм файли ўлчами 2 мартадан камаяди.

Кейинги босқич, расмни тронсформи бўлиб, JPEG учун Discrete Cosine Transform (DCT) фойдаланилади. Бундан ташқари Discrete Fourier Transform (DFT) ўзгартиришлари ҳам фойдаланилади. Бу метематик ўзгартиришлар расмни пикселларини ўзгартириш орқали амалга оширилади. DCT ўзгартиришларида расм кўринишидаги сигналлар частота шаклида ифодаланади. Бунда расмнинг 8x8 пиксел қисмлари бир блок сифатида олинади ва ўзгартириш натижаси ҳар бир блок учун 64 DCT коиффициентга тенг бўлади. Бир DCT коиффициентни ўзгариши 64 та расм пикселига таъсир этади.

Шундан сўнг, санаш (квантизация) жараёни амалга оширилади. Бу ерда инсон кўзининг бошқа бир хусусиятидан фойданилади. Яъни, инсон кўзи катта соҳадаги ёритилганликдаги кичкина фарқни яхши фарқлай олади. Аммо, юқори частотадаги ёритилганликдаги фарқларни ажратиш даражаси яхши эмас. Яъни, юқори частоталар кучини камайтириш орқали расмни ўзгармаслигини таъминлаш мумкин. JPEG буни блокдаги барча қийматларни квантлаш коиффициенти орқал бўлиш билан амалга оширади. Бу натижалар бутун қийматларга яхлитланади ва коиффицентларни Хаффан кодлаш

усулидан фойдаланиб ўлчамлари камайтирилади.

JPEG стегонографияси. Одатда стегонографияда JPEG файллардан йўқотиш орқали сиқиши сабабли фойдаланилмайди. Стегонографиянинг муҳим бир хусусиятларидан бири шуки хабарни контентнинг муҳим саналмаган битлари ўрнига қўйишдир. JPEG форматдан фойдаланилганда айнан шу муҳим саналмаган битлар ўзгариши натижасида, хабар бузулиши мумкин. Шунга қарамасдан сиқиш алгоритмларининг хусусиятларидан фойдаланиб, JPEG учун ҳам стегонографик алгоритм ишлаб чиқиш мумкин.

JPEG форматининг асосий хусусиятидан бири бу - сиқиш натижасидаги ўзгаришни инсон кўзи орқали аниқлаш имкони йўқлигидир. DCT фойдаланиб сиқишда, коифициентлардани ўзгаришга катта аҳамият қаратилмайди. Ушбу хусусият алгоритмни йўқолиш билан сиқишини таъминлаб қолмасдан, балки маълумотларни яшириш учун фойдаланилиши мумкин.

JPEG форати одатда йўқотилиш билан сиқиш усули сифатида қаралсада, унда йўқотилиш билан ва йўқотилишсиз амалга ошириш босқичлари мавжуд. DCT ва квантизация жараёнлари йўқотилишли босқичлар саналса, Хаффам усулида кодлаш эса йўқотилишсиз босқичдир. Стегонография ушбу босқичларнинг ўртасида жойлашиши лозим. Яъни, LSB усулида маълумотларни яшириш Хаффман кодлашидан олдин амалга оширилади. Бу усул орқали маълумотни яширганда, уни аниқлаш жараёни жуда қийин бўлади ва инсон кўзи орқали аниқлаш мумкин бўлмайди.

Бундан ташқари расм стегонографиясида юқоридаги иккита усулнинг комбинацион тарзда фойдаланишга асосланган усуллар ҳам мавжуд.

Patchwork. Юқоридаги усулларнинг комбинацяси асосида ишлаб сиқилган усуллардан биридир. Patchwork статистик технология саналиб, расмда хабарни бириктириш учун қолдиқ хабарни кодлашдан фойдаланилади. Алгоритм яширинувчи хабарга қолдиқ хабар қўшади ва уни расм бўйлаб ёяди. Псевдотасодифий сонлар генератори расмдан иккита тасодифик қисмни, А ва В қисмларни топишда фойдаланилади. А қисмдаги барча пикселлар ёритилади ва В томон қоронғулаштирилади. Бошқа сўз билан айтилганда, биринчи қисм бирор қийматда ёритилса, иккинчи қисм айнан шу қийматда қоронғулаштирилади. Бу қарама-қаршилик орқали бир бит маълумотни кодлаш мумкин бўлиб, расмнинг қолган қисми ўзгармас қолади.

Бу усулнинг камчилиги эса фақат бир битни яширишидир. Бирдан кўп битларни яшириш учун, расмларни кўплаб қисм расмларда ажратиш ва уларнинг ҳар бирида бир битдан маълумотларни яширилади. Бу усулнинг афзаллиги эса, махфий хабарни бутун контент (расм) бўйлаб тенг

ёйилишидир. Шунинг учун, расмнинг бир қисмдаги ўзгариш бошқа қисмларига таъсир этмайди.

Кенг спектрлар. Кенг спектрлар технологиясида яширинувчи маълумот контент (расм) буйлаб тарқатилади. Бу тизим Марвел томонидан таклиф этилган бўлиб, кенг спектрлар алоқаси, хатоликларни назоратлаш кодлари ва расм жараёнлари комбинациясидан иборат.

Кенг спектрлар алоқаси кенг полосали частоталарда кичик полосали частоталарни ёйиш билан характерланади. Бунинг натижасида кенг поласалардан керакли полосадаги частотани аниқлаш имкони йўқолади. Бу усулда асосланган расм стегонографиясида эса, хабар шовқинлар ичига киритилади ва кейин контент (расм) билан бириктиралади. Натижада махфий хабар яширинган контент ҳосил бўлади. Хабар шовқин маълумот ичига киритганлиги сабабли, уни аниқлаш қийинлашади. Хабарни аниқлашда ҳақиқий контент (ҳақиқий расм, хабар бириктирмадан олдинги ҳолати) зарур бўлиб, у бўлмаганда хабарни аниқлаш имкони мавжуд эмас.

Қуйидаги жадвалда расм стегонографиясидаги алгоритмларнинг таҳлили келтирилган.

12.1 - жадвал

	BMP да LSB	**GIF да LSB**	**JPEG сиқиш**	**Patchwork**	**Кенг спектрлар**
Кўринмаслик	Юқори	Ўртача	Юқори	Юқори	Юқори
Қўшимча қўшиладиган маълумот ҳажми	Юқори	Ўртача	Ўртача	Паст	Ўртача
Статистик таҳдидга бардошлилик	Паст	Паст	Ўртача	Юқори	Юқори
Расмни бузишга асосланган таҳдидга бардошлилик	Паст	Паст	Ўртача	Юқори	Ўртача
Файл форматига боғлиқлилик	Паст	Паст	Паст	Юқори	Юқори
Шубҳаланмаслик даражаси	Паст	Паст	Юқори	Юқори	Юқори

Назорат саволлари

1. Стегонотаҳлил усуллари.
2. Расм маълумотларда ахборотларни яшириш.
3. Ёқотилишли ва ёқотилишсиз сиқиш.

4. Муҳимлиги паст бит.

Фойдаланилган адабиётлар

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, (2008). Digital Watermarking and Steganography, the Morgan Kaufmann Series in Multimedia Information and Systems, 2nd Ed.
2. Peter Wayner, (2008). Disappearing Cryptography, Second Edition - Information Hiding: Steganography and Watermarking, Morgan Kaufmann.

Bruce Schneier, (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C, second Edition, John Wiley & Sons.