Dokaz vodnega žiga brez razkritja znanja

Miha Štajdohar

01.07.2008

Povzetek

Dokaz vodnega žiga brez razkritja znanja omogoča dokazovalcu, da razsodniku dokaže njegovo prisotnost med podatki, ne da bi ob tem razkril informacije, s katerimi bi ga lahko odstranili. V članku je predstavljena ideja Adelsbacha in Sadeghija, ki sta prva definirala tak protokol. Izpostavljeno je vprašanje varnosti in motivacije, ki nas vodi k dokazom vodnega žiga brez razkritja znanja.

1 Uvod

Zaščita digitalnih del proti zlorabi ali nezakoniti distribuciji je postala zahtevna naloga v informacijski skupnosti. Ker popolna zaščita proti zlorabi ni možna, se večina tehnik za zaščito avtorskih pravic osredotoča na zaznavanje napačnih uporab. Informacijo o identiteti avtorja neopazno skrijemo med originalne podatke s tehnikami vodnih žigov [5, 6, 7]. Občajno avtor pri dokazovanju prisotnosti vodnega žiga predloži informacije, ki bi jih lahko nekdo zlorabil za odstranitev vodnega žiga. Da bi dokazali prisotnost vodnega žiga, ne da bi ob tem razkrili občutljive informacije, uporabimo protokol dokazov brez razkritja znanja [1, 4].

Pri teh protokolih dokazovalec prepriča razsodnika, da pozna skrivnost, v našem primeru vodni žig, ob tem pa razsodnik ne izve ničesar novega o njej. Dokaz brez razkritja znanja je interaktivni kriptografski protokol med dokazovalcem, ki dokazuje svojo trditev, in razsodnikom, ki od dokazovalca zahteva dokaz. Dokaz brez razkritja znanja razsodniku pove le, ali je izjava pravilna ali ni. Teorijo interaktivnih dokazov in dokazov brez razkritja znanja je leta 1985 predstavil Shafi Goldwasser s sodelovci [8].

V članku bomo predstavili idejo vodnih žigov brez razkritja znanja, ki sta jo prva definirala Adelsbach in Sadeghi. Pred tem bomo opisali pojme, ki so potrebni za razumevanje omenjenega protokola, kot so: definicija in opis dokazov brez razkritja znanja, vodni žigi in sheme zaupanja. Ob koncu bomo preučili vprašanje varnosti, skozi članek pa bomo orisali motivacijo, ki nas vodi k dokazom vodnega žiga brez razkritja znanja.

2 Vodni žig

Označevanje z vodnim žigom je proces dodajanja informacij nekemu mediju, dodane podatke pa imenujemo vodni žig. Ime izhaja iz časov, ko so vodni žig tiskali na papir. Uporabljamo ga za zaščito avtorskih pravic, za digitalni prstni odtis, televizijski prenos in na mnogih drugih področjih. S tem želimo preprečiti nezakonito prepisovanje podatkov. V članku se bomo osredotočili na digitalno označevanje z vodnim žigom, ki obravnava digitalne medije. Informacijo torej vstavimo v digitalni signal. Poznamo dve vrsti označevanja z vodnim žigom. Prva je vidno označevanje, kjer je informacija vidna na sliki ali filmu. Običajno je to besedilo ali logotip, ki predstavlja avtorja oziroma lastnika medija. Druga vrsta, ki je za nas bolj pomembna, je nevidno označevanje z vodnim žigom. Informacije, ki jo dodamo mediju, človek ne more zaznati brez dodatne analize.

Signal z dodanim vodnim žigom običajno shranimo ali ga posredujemo drugi osebi. Poskus spremembe ali odstranitve vodnega žiga, čeprav ta ni vedno zlonamerna, imenujemo napad. Da bi zmanjšali število uspešnih napadov na vodne žige, želimo ob dokazovanju avtorstva izdati kar se da malo informacij. V zadnjem času je bilo narejenih veliko raziskav na temo dokaza vodnega žiga z orodjem dokazov brez razkritja znanja.

2.1 Definicija sheme vodnega žiga

Obstaja mnogo različnih definicij in notacij shem vodnih žigov. Tukaj bomo opisali tiste osnovne gradnike, ki jih bomo uporabili v naslednjih poglavjih.
Shema vodnih žigov z dokazovanjem vsebuje štiri algoritme, ki se izvedejo v polinomskem času:

1. GEN_KEY = $(k_{\text{emb}}, k_{\text{det}})$,
2. GEN_WM = WM,
3. EMBED(W, WM, k_{emb}) = W$''$ in
4. DETECT(W$''$, WM, W, k_{det}) $\in \{da, ne\}$

Prva dva sta verjetnostna algoritma in vrneta par ključev $(k_{\text{emb}}, k_{\text{det}})$ ter vodni žig (watermark, WM). Algoritem EMBED(W, WM, k_{emb}) s ključem k_{emb} nezaznavno vloži vodni žig WM v podatke, ki jih označimo z W. Rezultat algoritma so podatki z dodanim vodnim žigom W$''$. Algoritem DETECT(W$''$, WM, W, k_{det}) nam pove, ali podatki W$''$ vsebujejo vodni žig WM glede na referenčne podatke W z uporabo ključa k_{det}.

Da ne bi kdo prišel do originalnih podatkov W, je treba preverjati vodni žig tako, da jih (W) ob tem ne razkrijemo. Shemi s to zelo zaželeno lastnostjo pravimo *slepa shema*. Pokazali bomo, da je dokaz vodnega žiga brez razkritja znanja možno izvesti tako za shemo, ki ni slepa, kot tudi za tako, ki to je.

2.2 Coxova shema vodnega žiga

Osnova za dokaz vodnega žiga brez razkritja znanja, ki ga predpišeta Adelsbach in Sadeghi [1], je Coxova shema vodnega žiga [7]. Ta shema v svoji osnovni obliki ne uporablja ključa. Zasnovana je bila za slikovni material, a jo lahko z uporabo ustreznih preslikav posplošimo na poljubne podatke. Temelji na principu razpršenega spektra.

Ideja razpršenega spektra je bila originalno razvita za zaščitene radijske komunikacije. Tu je glavni problem podoben tistemu v zaščiti podatkov z vodnim žigom. Ozkopasovni signal (vodni žig) mora biti prenesen preko širokopasovnega kanala, ki je tarča šumov in popačenj (multimedijski podatki: video, avdio). Osnovni princip razpršenega spektra pri vodnih žigih je sestavljen iz naslednjih korakov:

- generiranje signala ponavljajočih se informacijskih bitov vodnega žiga in
- modulacija signala ponavljajočih se informacijskih bitov vodnega žiga s psevdo-šum signalom dobljenim iz generatorja naključnih števil.

Ponovna pridobitev vkodirane informacije o vodnem žigu je možna samo, če poznamo psevdo-šumni signal, ki je bil uporabljen za modulacijo. V Coxovi shemi izvedemo modulacijo z diskretno kosinusno transformacijo – DCT(W, k), izbrani psevso-šumni signal pa označimo s k. Formula diskretne kosinusne transformacije:

$$\text{DCT}(\text{W}, k) = \sum_{n=0}^{N-1} \text{W}_n \cos\left[\frac{\pi}{N}(n + \frac{1}{2})(k + \frac{1}{2})\right], \tag{1}$$

kjer je N število pomnilniških besed, ki predstavljajo originalne podatke W, ~~kjer~~ je W_n ena pomnilniška beseda. Algoritem GEN_WM zgradi vodni žig WM, ki je oblike:

$$\mathrm{WM} = (\mathrm{WM}_1, ..., \mathrm{WM}_k) \tag{2}$$

in je zaporedje realnih števil. Razporeditev števil vodnega žiga po originalnih podatkih določa njegova dolžina k. Algoritem EMBED vloži vodni žig WM v podatke, ki so pretvorjeni z diskretno kosinusno tranformacijo in so oblike:

$$\mathrm{DCT}(\mathrm{W}, k) = (\mathrm{DCT}(\mathrm{W}, k)_1, ..., \mathrm{DCT}(\mathrm{W}, k)_k) \tag{3}$$

Vodni žig vložimo z enačbo:

$$\mathrm{W}'' = \mathrm{DCT}(\mathrm{W}', k)_i := \mathrm{DCT}(\mathrm{W}, k)_i * (1 + \alpha * \mathrm{WM}_i), \tag{4}$$

kjer z α nastavljamo razmerje med robustnostjo (vodni žig se ohrani pri transformacijah slike) in nezaznavnostjo vodnega žiga v podatkih.

Kot bomo videli, algoritem za dokazovanje ne potrebuje referenčnih podatkov W. Vodni žig potrdimo z računanjem funkcije (coor), ki mora biti nad željenim pragom (corr $\geq \delta$).

Definirajmo simbol Δ kot razliko med DCT podatkov, ki vsebujejo vodni žig, in DCT originalnih podatkov:

$$\Delta = \mathrm{DCT}(\mathrm{W}'', k) - \mathrm{DCT}(\mathrm{W}, k) \tag{5}$$

V nadaljevanju bomo uporabili oznako $\langle \hat{x}, \hat{y} \rangle$ za običajen skalarni produkt vektorjev $\hat{x}$ in $\hat{y}$, $\|x\|$ pa za dolžino vektorja $\hat{x}$:

$$\|x\| = \sqrt{\langle x, x \rangle} \tag{6}$$

Korelacijo lahko v Coxovi shemi računamo na dva načina. Če jo računamo po enačbi:

$$\mathrm{corr} = \frac{\langle \Delta, \mathrm{WM} \rangle}{\|\Delta\|}, \tag{7}$$

shema ni slepa. Iz enačbe je razvidno, da pri dokazovanju potrebujemo originalne podatke W. Ker razkritje podatkov predstavlja varnostno grožnjo, raje uporabimo enačbo:

$$\mathrm{corr} = \frac{\langle \mathrm{DCT}(\mathrm{W}'', k), \mathrm{WM} \rangle}{\|\mathrm{DCT}(\mathrm{W}'', k)\|}. \tag{8}$$

V tem primeru je shema slepa, vendar se moramo zavedati, da je pri slepi shemi zaznavanje vodnega žiga manj robustno.

3 Dokaz brez razkritja znanja

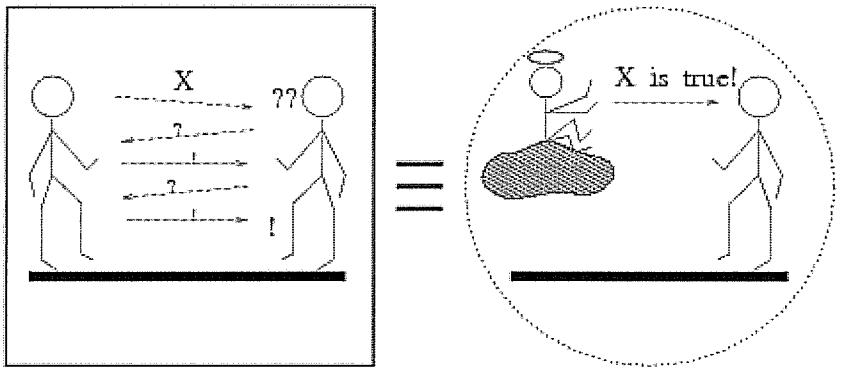
V kriptografiji s pojmom dokaz brez razkritja znanja označimo interaktivni kriptografski protokol, s katerim dokazovalec dokaže razsodniku resničnost neke trditve. Dokazovalec ob dokazovanju trditve same ne razkrije. Razsodniku dokaže le, da je resnična.

V kriptografiji dokaz brez razkritja znanja običajno poteka tako, da dokazovalec pozna rešitev nekega težkega matematičnega problema. Kot primer si lahko predstavljate faktorizacijo zelo velikega števila, ki je produkt dveh praštevil. Nato ga dokazovalec z naključno transformacijo pretvori v izomorfen problem. Dokazovalec pozna tudi rešitev tega problema, saj pozna tako naključno transformacijo kot rešitev originalnega problema. Razsodnik nato od dokazovalca zahteva enega[1] od dveh možnih dokazov:

[1] Če bi razsodnik izvedel odgovora na obe vprašanji, lahko ugotovi rešitev originalne trditve. To ni v interesu dokazovalca, ki želi, da trditev ostane skrita.

- dokaz, da sta oba problema izomorfna, oziroma
- rešitev novega (izomorfnega) problema.

Če dokazovalec pozna rešitev prvotnega problema, bo lahko odgovoril na obe vprašanji. Če rešitve ne pozna, lahko pravilno odgovori le na eno od dveh možnih vprašanj. Verjetnost, da bo odgovoril narobe, je torej 50%. Da se razsodnik prepriča v resničnost trditve, postopek ponavlja (Slika 1), dokler verjetnost ne pade na dovolj majhno vrednost. Verjetnost, da dokazovalec trditve ne pozna, pada eksponentno in po n korakih znaša 2^{-n}.



Slika 1: Interaktivno dokazovanje brez razkritja znanja.

Dokaz brez razkritja znanja mora zadoščati trem lastnostim:

1. **popolnost:** pošteni razsodnik je prepričan v resničnost trditve, kadar jo dokaže pošteni dokazovalec;
2. **razsodnost:** če je trditev neresnična, je verjetnost, da bi goljufivi dokazovalec prepričal poštenega razsodnika, neznatna;
3. **brez razkritja znanja:** če je trditev resnična, se lahko razsodnik nauči samo to, da je resnična. Torej ne izve ničesar novega o vsebini trditve.

Dokaz brez razkritja znanja ni dokaz v matematičnem smislu. Iz lastnosti razsodnosti sledi, da obstaja možnost, čeprav majhna, da dokazovalec prepriča razsodnika v resničnost svoje trditve, čeprav ta ne velja. Dokaz torej ni determinističen. Kljub temu se z uporabo dokaza brez razkritja znanja ta verjetnost zmanjša na zanemarljivo majhno.

3.1 Primer dokaza brez razkritja znanja

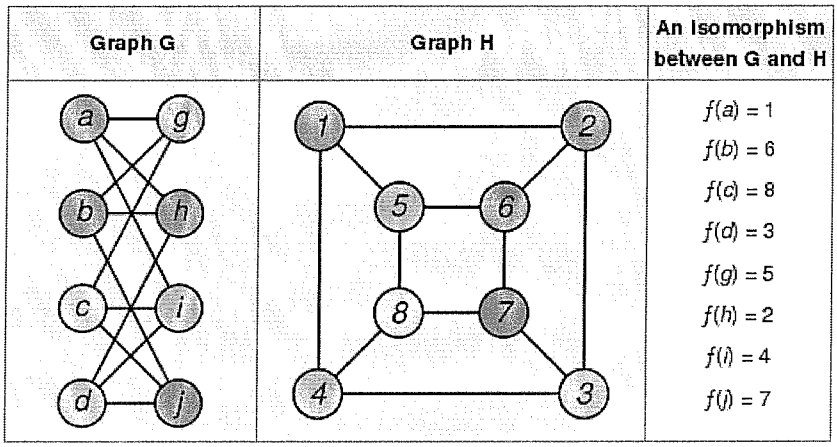
Dokaz brez razkritja znanja je najlažje razložiti na primeru z jamo Ali Babe [6]. Ker pa je za razumevanje dokaza vodnih žigov brez razkritja znanja potrebno spoznati nekatere matematične lastnosti, si oglejmo primer z grafi. Dokaz brez razkritja znanja lahko uporabimo na poljubnemu NP-polnemu problemu in nekaterimi drugimi težkimi problemi.

Dokazovalec Denis pozna Hamiltonov cikel (cikel, ki v grafu G vsako točko obišče natanko enkrat). Razsodnik Robert pozna graf G, ne pozna pa cikla. Denis bi mu rad dokazal, da je v grafu našel Hamiltonovo pot, ne da bi mu jo pokazal ali izdal kakšno drugo informacijo. Robert je lahko potencialni kupec te informacije in bi se rad prepričal, da jo dokazovalec res pozna. Morda je Denis edini, ki pozna to informacijo in bi rad s tem dokazal svojo identiteto.
Dokaz poteka iterativno s ponavljanjem zaporedja korakov.

- Na začetku vsake iteracije Denis zgradi graf H, ki je izomorfen grafu G (Slika 2). Izomorfizem grafov je bijektivna preslikava točk iz množice G v H tako, da sta za dve sosednji

točki u in v grafa G, sosednji tudi njuni sliki $f(u)$ in $f(v)$ v grafu H. Prevesti Hamiltonov cikel na graf H je trivialno, saj poznamo prepis za preslikavo vsake točke. Če Denis pozna Hamiltonov cikel v grafu G, ga pozna tudi v H.

- Denis pošlje graf H Robertu.
- Robert naključno postavi eno od dveh vprašanj. Denisa lahko vpraša, naj mu pokaže izomorfizem, ki si ga je zbral, ali pa naj mu pokaže Hamiltonov cikel na novem grafu.
- Če ga Robert vpraša o izomorfizmu, mu mora Denis pokazati matriko preslikave točk iz grafa G v H.
- Če pa ga vpraša o Hamiltonovem ciklu, Denis prevede svoj Hamiltonov cikel iz grafa G na H in ga pokaže Robertu, ki lahko preveri veljavnost cikla.



Slika 2: Primer izomorfnih grafov.

Dokler ne objavi grafa H, Denis ne ve, kaj ga bo vprašal Robert. Da je torej sposoben odgovoriti na obe vprašanji, mora biti graf H izomorfen G in poznati Hamiltonovo pot v H. Ker lahko na obe vprašanji vedno odgovori pravilno le nekdo, ki pozna Hamiltonov cikel v G, postane Robert po dovolj ponovitvah postopoma prepričan, da Denis govori resnico.

Denisov odgovor ne razkrije originalnega Hamiltonovega cikla v G. Robert vedno zve le odgovor na eno od vprašanj. Da bi lahko ugotovil prvotni cikel, bi potreboval odgovor na obe vprašanji. Robert, čeprav pozna grafa G in H, v realnem času ne more izračunati izomorfizma, ker je to NP-poln problem. Informacija torej ostane skrita, če si Denis v vsaki iteraciji zamisli drugačen graf H, izomorfen G.

Če Denis v resnici ne bi poznal Hamiltonovega cikla, bi lahko ugibal, katero vprašanje ga bo Robert vprašal. Poslal bi mu ali izomorfen graf H, v katerem cikla ne pozna, ali pa nek neizomorfen graf, v katerem tak cikel pozna. Z ugibanjem je verjetnost, da bi Denis ukanil Roberta, enaka 2^{-n}, kjer je n število iteracij.

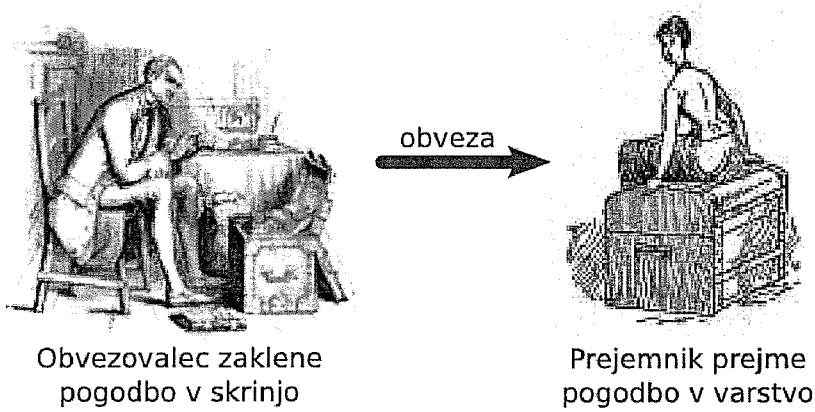
4 Dokaz vodnega žiga brez razkritja znanja

Motivacija za dokaz vodnega žiga izhaja iz običajnih shem za označevanje z vodnimi žigi, kjer prisotnost vodnega žiga potrjuje lastninske pravice. Vse te sheme se soočajo z isto težavo. Da lahko dokazovalec dokaže prisotnost svojega vodnega žiga, mora razkriti občutljive informacije razreševalcu spora, ki ni nujno zaupanja vredna oseba. V večini primerov ti podatki zadostujejo za odstranitev vodnega žiga.

Dokaz vodnega žiga brez razkritja znanja rešuje to varnostno grožnjo. Dokazovalcu omogoča, da dokaže prisotnost svojega vodnega žiga, ne da bi razkril kakršne koli informacije o njem, referenčnih podatkih ali ključu.

4.1 Sheme zaupanja

Shemo zaupanja si lahko predstavljamo kot interakcijo med dvema osebama (obvezovalec in prejemnik), kjer obvezovalec zaklene pogodbo v zaboj in ga da v varstvo prejemniku (Slika 3). Obvezovalec pogodbe, ki je v zaboju, ne more spremeniti, ker je zaboj v varstvu prejemnika in do nje nima dostopa. Tudi prejemnik pogodbe ne more spremeniti, ker nima ključa. Kasneje lahko obvezovalec razkrije vsebino pogodbe, če je to potrebno.

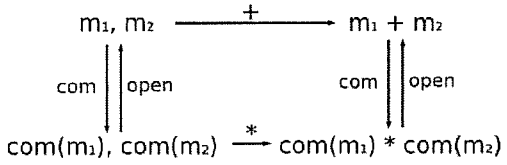


Slika 3: Primer sheme zaupanja.

Shema zaupanja je metoda, ki omogoča obvezovalcu, da *obveže* neko vrednost. Z obvezo (ang. commitment) vrednost skrijemo. Dokler je obvezana, se tudi ne more spremeniti. Obvezovalec jo lahko razkrije kasneje.

Shema zaupanja je protokol med dvema strankama. Sestavlja ga funkcija $\mathrm{com}(m, \mathrm{par}_{\mathrm{com}})$, s katero obvežemo (ang. commit) neko sporočilo $m \in M$, kjer je M končna množica sporočil. Običajno sporočilo m obvežemo tako, da ga šifriramo. Poleg funkcije com vsebuje shema zaupanja tudi funkcijo $\mathrm{open}(m, \mathrm{par}_{\mathrm{com}}, \mathrm{sk}_{\mathrm{com}})$, ki obvezo razveže (ang. open) v originalno sporočilo m. Obveza in razveza sta inverzni operaciji. S simbolom $\mathrm{par}_{\mathrm{com}}$ označimo vse javne parametre, ki jih potrebujemo za obvezo, s $\mathrm{sk}_{\mathrm{com}}$ pa zasebno informacijo obvezovalca, s katero obvezo razdre. Običajno pišemo le com() in open().

Da lahko izkoristimo tehniko dokazov brez razkritja znanja, mora v shemi zaupanja veljati naslednji homomorfizem (Slika 4): naj bosta $\mathrm{com}(m_1)$ in $\mathrm{com}(m_2)$ obvezi sporočil $m_1, m_2 \in M$. Potem lahko obvezovalec razdre $\mathrm{open}(\mathrm{com}(m_1) * \mathrm{com}(m_2))$ v $m_1 + m_2$ in ob tem ne razkrije nič informacije o $\mathrm{com}(m_1)$ oziroma $\mathrm{com}(m_2)$.



Slika 4: Homomorfizem, ki mora veljati v shemi zaupanja.

S stališča varnosti mora za shemo zaupanja veljati:

- ko je sporočilo obvezano, ga nepošteni obvezovalec ne more razdreti (razvezati) v drugačno sporočilo $m' \neq m$ kot v tisto, ki je bilo obvezano;
- obveza sporočila m ne izda prejemniku nobene informacije o m.

V opisu protokola *dokaz vodnega žiga brez razkritja znanja* bomo uporabili primer sheme zaupanja iz [9]: naj bo n produkt dveh praštevil p in q, naj bosta g in h generatorja ciklične podgrupe G iz $\mathbb{Z}_n^*$ reda $\frac{p-1}{2}\frac{q-1}{2}$ in naj bo $\text{par}_{\text{com}} = (n, g, h)$. Faktorizacija števila n in diskretna logaritma $\log_g h$ ter $\log_h g$ ne smeta biti znana prejemniku. Obvezovalec obveže vrednost $m \in M = \{0, ..., n-1\}$ tako, da izračuna $\text{com}(m, \text{par}_{\text{com}}) := g^m h^r \mod n$, kjer je $\text{sk}_{\text{com}} = r$ naključno izbrano naravno število na intervalu $[0, 2^l n)$ in je l reda velikosti bitne dolžine n.

4.2 Definicija dokaza vodnega žiga brez razkritja znanja

Za razliko od Coxove sheme so v našem primeru koeficienti vodnega žiga in tranformacije DCT cela števila. Enačbo (7) zapišemo kot

$$C := \underbrace{(\langle \Delta, \text{WM} \rangle)}_{A}^2 - \underbrace{\langle \Delta, \Delta \rangle * \delta^2}_{B} \geq 0 \tag{9}$$

in enačbo (8) kot

$$F := \underbrace{(\langle \text{DCT(W"}, k), \text{WM} \rangle)}_{D}^2 - \underbrace{\langle \text{DCT(W"}, k), \text{DCT(W"}, k) \rangle * \delta^2}_{E} \geq 0, \tag{10}$$

kjer je $\delta = \text{corr}$. Zapis je ekvivalenten enačbama (7) in (8), če sta vrednosti izrazov A in D nenegativni.

Naj bo (com, open) varna shema zaupanja. Dokaz vodnega žiga brez razkritja znanja – ZK_DETECT za shemo vodnega žiga (GEN_KEY, GEN_WM, EMBED, DETECT) je protokol med dokazovalcem P in razsodnikom V. Običajni vhodni podatki so:

- podatki z dodanim vodnim žigom W″,
- obveza vodnega žiga com(WM),
- obveza originalnih podatkov com(W),
- obveza parametra k_{wm} $\text{com}(k_{\text{wm}})$ in
- javni parametri $\text{par}_{\text{com}} = (\text{par}_{\text{com}}^{\text{WM}}, \text{par}_{\text{com}}^{\text{W}}, \text{par}_{\text{com}}^{k_{\text{wm}}})$ za dane obveze.

Privatni vhodni podatek dokazovalca je:

- zasebna informacija dokazovalca s katero zavezo razdre $\text{sk}_{\text{com}} = (\text{sk}_{\text{com}}^{\text{WM}}, \text{sk}_{\text{com}}^{\text{W}}, \text{sk}_{\text{com}}^{k_{\text{wm}}})$.

Oseba P dokaže, da pozna n-terico $(\text{WM}, \text{W}, k_{\text{wm}}, \text{sk}_{\text{com}}^{\text{WM}}, \text{sk}_{\text{com}}^{\text{W}}, \text{sk}_{\text{com}}^{k_{\text{wm}}})$ tako, da dokaže, da velja enačba:

$$\begin{aligned}(\text{open}(\text{com}(\text{WM}), \text{par}_{\text{com}}^{\text{WM}}, \text{sk}_{\text{com}}^{\text{WM}}) = \text{WM}) \wedge \\ (\text{open}(\text{com}(\text{W}), \text{par}_{\text{com}}^{\text{W}}, \text{sk}_{\text{com}}^{\text{W}}) = \text{W}) \wedge \\ (\text{open}(\text{com}(k_{\text{wm}}), \text{par}_{\text{com}}^{k_{\text{wm}}}, \text{sk}_{\text{com}}^{k_{\text{wm}}}) = \text{W}) \wedge \\ \text{DETECT}(\text{W}'', \text{WM}, \text{W}, k_{\text{wm}}) = \text{true}.\end{aligned}$$

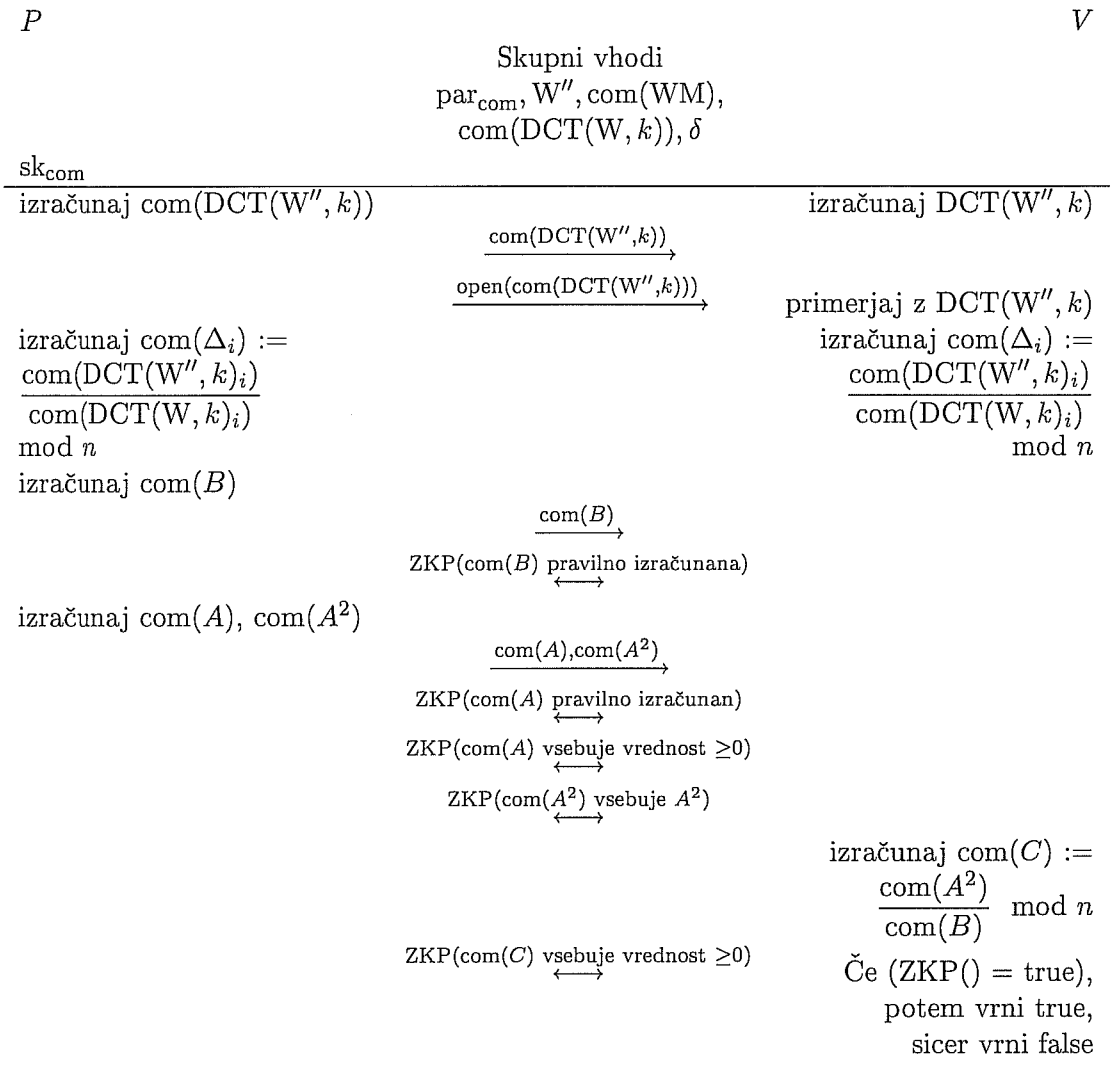
Protokol pove razsodniku ali naj sprejme vodni žig dokazovalca ali ne.

4.3 Dokaz vodnega žiga brez razkritja znanja, ki ni slep

Skupni vhodi dokazovalca P (ang. prover) in razsodnika V (ang. verifier) so: paramteri par_{com}, podatki z vodnim žigom W'', obvezan vodni žig po shemi zaupanja com(WM), obvezana diskretna kosinusna transformacija originalnih podatkov com(DCT(W, k)) in δ. Naj bo sk_{com} privatni vhod dokazovalca. Upoštevati moramo, da parametra Δ za razliko od transformacije $\text{DCT}(\text{W}'', k)$ v slepem protokolu ne smemo razkriti razsodniku, saj bi iz njega lahko izračunal diskretno kosinusno transformacijo originalnih podatkov DCT(W,k) ter iz nje pridobil podatke, ki ne vsebujejo vodnega žiga.

Zato oseba P korakoma izračuna vrednosti B in A, ju obveže in pošlje V. Nato brez razkritja znanja dokaže (ang. zero knowledge proof – ZKP), da za obvezane vrednosti drži relacija v enačbi (9). Z več dokazi skupaj (slika 5) dokažejo, da sta obvezi com(A) in com(B) izračunani pravilno iz obvez com(Δ) in com(WM). Sedaj oseba P brez razkritja znanja (ZKP) dokaže osebi V, da je obveza com(A) nenegativna. Oseba P izračuna obvezo com(A^2) in dokaže, da obveza vsebuje kvadrat vrednosti A.

Z uporabo homomorfizma osebi P in V izračunata obvezo com(C). Na koncu oseba P uporabi protokol brez razkritja znanja, da dokaže, da obveza com(C) vsebuje pozitivno vrednost.



Slika 5: Protokol dokaza brez razkritja znanja, ki ni slep.

4.4 Dokaz vodnega žiga brez razkritja znanja - slep

Slep protokol dokaza vodnega žiga brez razkritja znanja je podoben prejšnjemu. V slepem dokazu vodnega žiga brez razkritja znanja dokazovalec P dokaže razsodniku V, da je vodni žig, ki je shranjen v obvezi com(WM), prisoten v podatkih W''. Ob tem ne razkrije nikakršnega znanja o vodnem žigu WM. Protokol je prikazan na sliki 6.

P		V
	Skupni vhodi par_{com}, W'', com(WM), δ	
sk_{com}		
izračunaj DCT(W'', k)		izračunaj DCT(W'', k)
izračunaj E in com(E)		izračunaj E
	com(E) $\longrightarrow$	
	open(com(E)) $\longrightarrow$	primerjaj z E
izračunaj com(D) := $\prod_{i=1}^{k} \text{com}(\text{WM}_i)^{\text{DCT}(\text{W}'',k)_i} \bmod n$		izračunaj com(D) := $\prod_{i=1}^{k} \text{com}(\text{WM}_i)^{\text{DCT}(\text{W}'',k)_i} \bmod n$
	ZKP(com(D) vsebuje $D \geq 0$) $\longleftrightarrow$	
izračunaj com(D^2)		
	com(D^2) $\longrightarrow$	
	ZKP(com(D^2) vsebuje D^2) $\longleftrightarrow$	
izačunaj com(F) := $\frac{\text{com}(D^2)}{\text{com}(E)} \bmod n$		izačunaj com(F) := $\frac{\text{com}(D^2)}{\text{com}(E)} \bmod n$
	ZKP(com(F) vsebuje $F \geq 0$) $\longleftrightarrow$	
		Če (ZKP() = true), potem vrni true, sicer vrni false

Slika 6: Slepi protokol dokaza brez razkritja znanja.

Osebi P in V izračunata diskretno kosinusno transformacijo DCT podatkov W'', DCT(W'', k). Potem obe izračunata vrednost E po enačbi (10). Oseba P pošlje obvezo com(E) osebi V in jo takoj razdre. Oseba V se prepriča, da funkcija com(E) res vsebuje vrednost E. Obvezo com(E) bo oseba V potrebovala kasneje za izračune, a je sama ne more izračunati. Sedaj obe izračunata obvezo po enačbi:

$$\text{com}(D) := \prod_{i=1}^{k} \text{com}(\text{WM}_i)^{\text{DCT}(\text{W}'',k)_i} \mod n. \tag{11}$$

Oseba P z uporabo homomorfizma sheme zaupanja brez razkritja znanja dokaže, da je vrednost D nenegativna, kar je bil pogoj, da smo lahko uporabili enačbo (10).

Nato oseba P izračuna vrednost D^2 in pošlje osebi V obvezo com(D^2). Brez razkritja znanja ji dokaže (ZKP), da obveza res vsebuje kvadrat vrednosti, ki je zaklenjena v com(D). Ko sta prepričana, da obveza com(D^2) res vsebuje D^2, osebi P in V izračunata obvezo

$$\text{com}(F) := \frac{\text{com}(D^2)}{\text{com}(E)} \mod n \tag{12}$$

vrednosti F. Na koncu še oseba P dokaže osebi V brez razkritja znanja, da je vrednost, ki je vsebovana v com(F), nenegativna.

5 Varnost

Dokaz vodnega žiga brez razkritja znanja odpravlja ključno varnostno grožnjo obstoječih shem vodnih žigov: kdor želi dokazati prisotnost svojega vodnega žiga v podatkih, mora razkriti občutljive informacije (vodni žig, referenčne podatke ali zaznavni ključ), ki so potrebne pri ugotavljanju lastništva. Te informacije lahko v večini primerov zlorabimo za odstranitev vodnega žiga. V našem primeru (dokaz vodnega žiga brez razkritja znanja) teh informacij ne potrebujemo.

Dokaz brez razkritja znanja mora zadoščati trem lastnostim, ki so opisane v poglavju 3. Za zgoraj opisana protokola, ki uporabljata ZKP, morajo prav tako veljati omenjene lastnosti:

- popolnost,
- razsodnost in
- brez razkritja znanja.

Popolnost je lahko preverljiva. Če izjava ni resnična, je v obeh shemah dokazovalec ne more dokazati kot resnično. Iz tega sledi, da je razsodnik prepričan v resničnost trditve, ko mu jo dokazovalec dokaže.

Razsodnost drži. Dokazovalec P lahko goljufa le pri računanju obveze com(C) ali pri dokazovanju, da obveza com(C) vsebuje pozitivno vrednost. Vendar s tem razsodnost ne more veljati vsaj za enega od vsebovanih protokolov ZKP(), ker je verjetnost, da bi s protokolom ZKP dokazali neresnično trditev, neznatna.

Za protokol velja tudi lastnost *brez razkrija znanja*. Ob dokazu se namreč ne izda nobena nova informacija o vodnem žigu WM, ker so tudi vsi vsebovani protokoli ZKP() in ker so vrednosti WM, A in C varno skriti v obvezah.

Varnost je torej pogojena s shemo zaupanja. V opisanih protokolih uporabljamo shemo zaupanja iz [9]. Fujisaki in Jakamoto sta v članku [9] dokazala, da je shema računsko varna. Pri dokazu računske varnosti sta Fujisaki in Jakamoto uporabila predpostavko, da ni možno v polinomskem času izračunati faktorizacije števila n, ki je produkt dveh velikih praštevil p in q. Varnost je torej odvisna od trenutnega stanja na področju faktorizacije.

6 Zaključek

Predstavili smo protokol dokaza vodnega žiga brez razkritja znanja, ki je prvi dokazano varen. Zgrajen je na temeljih Coxove sheme vodnega žiga. Pokazali smo, da lahko z uporabo dokaza brez razkritja znanja varno in pravilno dokažemo prisotnost našega vodnega žiga. Ob tem ne razkrijemo novih informacij in s tem izboljšamo varnost vodnega žiga. Poveča se tudi uporabnost, saj lahko sedaj lastništvo ugotavlja tudi stranka, ki ji ne zaupamo brezpogojno.

Literatura

[1] A. Adelsbach and A. R. Sadegi, Zero-Knowledge Watermark Detection and Proof od Ownership, LNCS, volume 2137, 2001, pp. 273-288.

[2] S. Goldwasser, S. Micali and C. Rackoff, The knowledge complexity of interactive proof systems, SIAM J. Comput., volume 18, 1989, pp. 186-208.

[3] A. Adelsbach, M. Rohe, A. R. Sadeghi, Overcoming the obstacles of zero-knowledge watermark detection, Proceedings of the 2004 workshop on Multimedia and security, September 20-21, 2004, Magdeburg, Germany.

[4] O. Goldreich, S. Micali, A. Wigderson, Proofs that yield nothing but their validity, Journal of the ACM, volume 38, issue 3, pp. 690-728. July 1991.

[5] M. Ben-Or, O. Goldreich, S. Goldwasser, J. Hastad, J. Kilian, S. Micali, and P. Rogaway, Everything provable is provable in zero-knowledge, S. Goldwasser, editor, In Advances in Cryptology–CRYPTO '88, volume 403 of Lecture Notes in Computer Science, Springer-Verlag, 1990, 21-25. August 1988.

[6] J.-J. Quisquater, L. C. Guillou, T. A. Berson, How to Explain Zero-Knowledge Protocols to Your Children, Advances in Cryptology - CRYPTO '89: Proceedings, v.435, 1990, pp. 628-631.

[7] I. Cox, J. Kilian, T. Leighton and T. Shamoon, "A secure, robust watermark for multimedia", in Proc. Workshop on Information Hiding, Univ. of Cambridge, U.K., May 30 - June 1, 1996, pp. 175-190.

[8] S. Goldwasser, S. Micali and C. Rackoff, The Knowledge Complexity of Interactive Proof - Systems, Proceedings of STOC '85, 1985, pp. 291-304

[9] E. Fujisaki and T. Okamoto, Statistical Zero-Knowledge Protocols to Prove Modular Polynomial Relations, Crypto '97, LNCS 1294, Springer-Verlag, Berlin 1997, pp. 16-30