RAPORT ŞTIINŢIFIC FINAL

Contribuții la marcarea reversibilă în domeniul criptat

7.08.2020 – 31.07.2022

Proiectului „Contribuții la marcarea reversibilă în domeniul criptat” (CREED - *Contributions to REversible data hiding in the Encrypted Domain*) a urmărit realizarea de noi metode de inserție reversibilă pentru domeniul criptat, concentrându-se pe inserția în imagini digitale. S-a investigat și adaptarea metodelor pentru alte tipuri de date (cum ar fi fișiere audio). Metodele de inserția reversibilă în domeniul criptat sunt clasificate în două subcategorii în funcție de când se generează pentru informația ascunsă: înainte sau după criptarea fișierului gazdă (VRBE – *Vacating room before encryption* și respectiv VRAE – *Vacating room after encryption*).

În acest proiect s-au desfășurat trei etape corespunzătoare cu obiective principale ale proiectului: „Noi metode VRAE de inserție reversibilă de date” (etapa I), „Noi metode VRBE de inserție reversibilă de date” (etapa a II-a) și „Algoritm general de inserție reversibilă de date” (etapa a III-a).

1. Dezvoltarea de noi metode de inserție bazate pe principiul VRAE

Primul obiectiv (corespunzător etapei I) a fost îndeplinit prin crearea a doi algoritmi de inserție prin VRAE. Ambele abordări pornesc de la metoda introdusă în [1]: predicția independentă a pixelilor (prelucrarea unui pixel nu afectează predicția celorlalți pixeli gazdă) și gruparea lor aleatoare pe bază de cheie secretă (un bit ascuns fiind inserat în fiecare grupă).

Primul algoritm VRAE propus folosește predicția multiplă introdusă în [2] pe un context de predicție extins la 16 pixeli pentru prima etapă de inserție și 18 pixeli la etapă doi (figura 1). Este important de menționat că în [2] contextul de predicție constă este de 4 pixeli. La predicție se folosesc o versiune modificată a celor patru sub-predictorilor ce stau la bază predicției EGBSW [3].

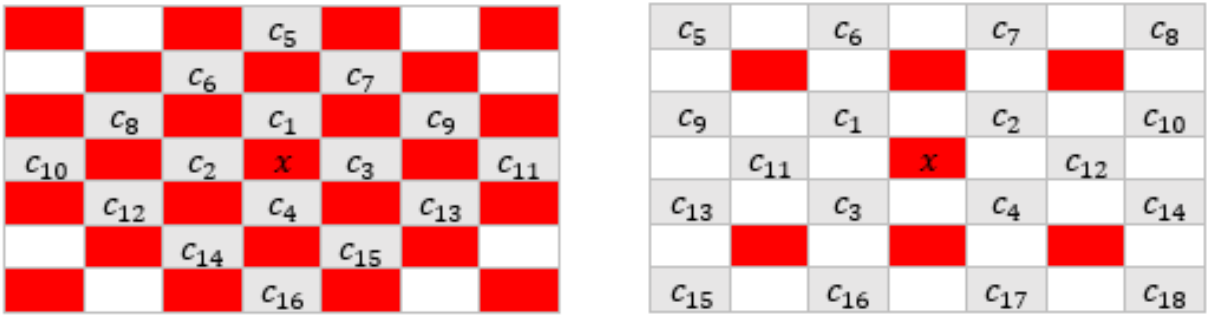

Figura 1. Contextul de predicție folosit de primul algoritm VRAE propus pentru etapa 1 (a) și etapa 2 (b) de inserție

Primii doi sub-predictori folosesc cei mai apropiați pixeli de pe o direcție (orizontală/verticală pentru etapa 1 și cele două diagonale pentru etapa 2):

$$\hat{x}_1 = \frac{c_1+c_4}{2} \qquad \hat{x}_2 = \frac{c_2+c_3}{2}$$

Ceilalți doi predictori folosiți depind de etapa curentă de inserție. La prima etapă, aceștia sunt calculați ca o medie ponderată între valoarea dată de o diagonală și valorile pe orizontală și verticală:

$$\hat{x}_3 = \frac{\frac{c_1+c_2+c_6+c_8}{2} + \frac{c_3+c_4+c_{13}+c_{15}}{2} + c_1+c_2+c_3+c_4}{8}$$

$$\hat{x}_4 = \frac{\frac{c_1+c_3+c_7+c_9}{2} + \frac{c_3+c_4+c_{12}+c_{14}}{2} + c_1+c_2+c_3+c_4}{8}$$

Etapa doi folosește o structură similară, însă valorile corespunzătoare direcției orizontale/verticale au ponderea cea mai mare în medie:

$$\hat{x}_3 = \frac{2\frac{c_1+c_3+c_{11}}{3} + 2\frac{c_2+c_4+c_{12}}{3} + c_1+c_2+c_3+c_4}{8}$$

$$\hat{x}_4 = \frac{\frac{c_1+c_2+c_6+c_7}{2} + \frac{c_3+c_4+c_{16}+c_{17}}{2} + c_1+c_2+c_3+c_4}{8}$$

Noua metodă VRAE oferă un raport mai bun capacitate/distorsiune comparativ cu [2] sub aceeași constrângere asupra ratei de decodare fără erori. Obținându-se un câștig mediu în PSNR de aproximativ 0.5 dB și o creștere în capacitate de până la 10.000 de biți.

Al doilea algoritm VRAE propus constă împărțirea imaginii în blocuri de pixeli și inserția pe bazată pe selecția aleatoare a blocurilor. Acesta a fost implementat într-o

versiune inițială în etapa 1 și finalizat în etapa 2. Inițial, această abordare părea mai limitată decât cea cu grupe de pixeli (folosită de algoritmul anterior discutat mai sus). Gruparea pixelilor în blocuri tinde să grupeze împreună pixeli din regiunile complexe ale imaginii (zone cu texturi cu aspect local aleator). Pixelii din aceste regiuni sunt dificil de estimat, eroarea de predicție este mare, iar predictorul poate selecta la decodare valoarea greșită. Gruparea acestor pixeli duce la decodarea eronată a întregului bloc. Soluția la această problemă constă în gruparea pe blocuri pentru predicție (astfel se maximizează capacitatea oferită de metodă) și crearea unor noi grupe pentru inserția de date. Astfel pixelii problemă sunt redistribuiți aleator împreună cu pixelii din regiuni mai ușor de prezis (zone uniforme sau cu contururi bine definite).

La această metodă, imaginea gazdă este împărțită în blocuri de $(n+1) \times (n+1)$ pixeli. Blocurile propuse sunt prezentate în figura 2. Dimensiunile testate pentru blocuri au fost între 20×20 si 50×50 de pixeli, în funcție de complexitatea imaginii și minimizarea ratei de eroare. Algoritmul procesează împreună k blocuri, prima grupa de pixeli se realizează cu pixelii de pe poziția 1 din cele k blocuri (pixelii x_1,1 în figura 1.c). Se alege pentru un strat de biți pentru inserție.

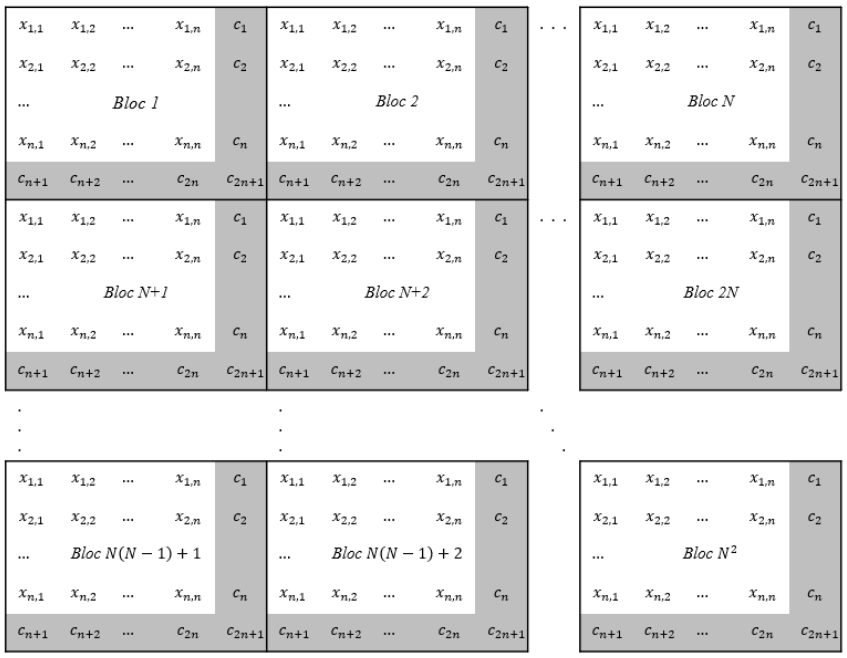

Figura 2. Distribuția pixelilor marcabili x_i și a contextului de predicție format din pixelii c_i pentru noua abordare VRAE bazată pe blocuri de pixeli

Predicția nu folosește valori din exteriorul blocului curent, astfel imaginea poate fi parcursă pe blocuri în orice ordine. Se folosește o cheie secretă de inserție pentru a genera ordinea de selecție a blocurilor pentru etapa de inserție a datelor. Această abordare permite permutarea blocurilor în etapa de criptare, crescând astfel securitatea imaginii gazdă, un avantaj față de [1], [2] și algoritmul anterior.

Metoda procesează simultan *k* blocuri citite în ordinea dată de cheia secretă. Pe baza celor *k* blocuri se creează n^2 grupe de pixeli. Prima grupa conține pixelii de pe poziția 1 din cele *k* blocuri (pixelii $\mathrm{x}_{1,1}$ în figura 2). Se inserează un bit ascuns în prima grupă prin negarea biților de pe un strat selectat (stratul ales controlează puterea inserției, care la rândul ei determină rate de eroare și distorsiunea introdusă în gazdă). După procesarea grupei 1, se formează grupa 2 ce conține toți pixelii $\mathrm{x}_{1,2}$. Procesul se repetă, ultima grupă conține pixelii $\mathrm{x}_{\mathrm{n,n}}$. La decodare, grupele sunt procesate în ordine inversă. Prima grupa restaurată la valorile inițiale este cea cu $\mathrm{x}_{\mathrm{n,n}}$, acești pixeli sunt apoi folosiți la predicția pixelilor $\mathrm{x}_{\mathrm{n-1,n}}$, care la rândul lor vor fi folosiți pentru predicția celorlalte grupe.

S-a investigat și adaptarea acestei metode pentru VRBE. Această adaptare constă în introducerea unei etape de preprocesare în care se identifică pixelii problemă (ce produc erori la decodare din cauza unei predicții slabe). Pozițiile acestor pixeli sunt memorate într-o hartă care este apoi compresată și inserată într-o zonă rezervată a imaginii (ce nu poate fi folosită direct la inserție). Harta este folosită la decodare pentru a restaura corect pixelii problemă (algoritmul selectează dintre două valori posibile pe baza predictorului, la pozițiile stocate în hartă se folosește valoarea opusă de cea indicată de predictor). Etapa de preprocesare elimină nevoia de insera în grupe de pixeli, capacitatea de inserție a algoritmului ajungând la 0.8 - 1 bpp (bit-per-pixel), în funcție de dimensiunea blocurilor alese.

În etapa 1 a proiectului s-a investigat abordării PVO (*pixel-value-ordering)* pentru domeniul criptat pornind de la metoda propusă în [4], metodele PVO fiind intens folosite în domeniul necriptat. S-a dezvoltat inițial **o noua abordare la inserția PVO în imagini necriptate**, mai exact s-a propus o noua parcurgere sub formă de șir vectorial a pixelilor gazdă. Această parcurgere elimină parcurgerea pe blocuri la PVO. Împărțirea unui șir în sub-șiruri de mărimi diferite este trivială comparativ cu împărțirea unei imagini (bidimensională) în blocuri de diverse dimensiuni fără a compromite calitatea blocurilor (și reversibilitatea metodei). La domeniul criptat, metoda din [4] s-a dovedit a fi ineficientă comparativ cu

metodele VRBE bazate pe predicție și/sau compresie (cum ar fi [5]). Însă metoda dezvoltată prezintă interes în domeniul necriptat, unde inserția PVO este un subiect intens cercetat ([6]). Pentru a fi competitivă, această metodă trebuie să fie adaptată la o structură PVO mai nouă decât cea implementată în prezent.

S-a cercetat și folosirea rețelelor de tip *deep learning* pentru predicție la VRAE și VRBE, însă rezultatele obținute au fost similare cu predictorii existenți în domeniu. Limitele impuse asupra contextului de predicția pentru menținerea reversibilității în domeniul criptat slăbesc rezultatele predicției pe bază de învățare. Astfel, folosirea unui predictor complex bazat pe nu este justificată la inserția reversibilă în domeniul criptat.

2. Dezvoltarea de noi metode de inserție bazate pe principiul VRBE

Al doilea obiectiv (corespunzător etapei II) a fost îndeplinit prin crearea a trei algoritmi de inserție prin VRBE. **Primul algoritm VRBE propus** are la baza algoritmul 2 VRAE descris în secțiunea anterioară. Avantajul principal față de alte abordări din domeniu este permutarea blocurilor la criptare ce poate fi realizată independent de ordinea de inserție a datelor ascunse. Algoritmii VRBE curenți nu folosesc permutarea blocurilor [5] sau au nevoie de o criptare specială pentru a indica natura blocurilor ce pot conține date [7].

A doua metodă, **inserția reversibilă prin PEE cu substituție de LSB** introduce nou set de ecuații de inserție care permit înlocuirea valorii LSB pentru fiecare pixel selectat pentru inserție (indiferent dacă aceasta este clasificat ca inserabil, deplasabil sau cu risc de depășire).

Algoritmul propus împarte imaginea gazdă în două regiuni. Prima regiune are un număr de pixeli egal cu capacitatea dorită (măsurată în biți). Noile ecuații de sunt folosite pentru această regiune. Biții sunt inserați în toți pixelii din această regiune. Pixelii inserabili pot fi decodați fără a avea nevoie de informații suplimentare. La pixeli deplasabili și la cei cu risc de deplasare este nevoie să se stocheze LSB-urile originale sub formă de date auxiliare. A doua regiune este folosită pentru inserția datelor auxiliare și folosește ecuațiile clasice de inserție prin PEE. Abordarea propusă este extrem de flexibilă, deschizând calea pentru o serie noua de metode de inserție atât pe domeniul criptat cât și pe cel clasic.

A treia metodă, **VRBE prin substituție de MSB în imagini RGB și fișiere audio**, pornește de la inserția reversibilă propusă în [5]. Pentru imaginile color se folosesc straturi derivate ca referințe pentru predicție:

$$U = R - G$$
$$V = B - G$$

Predicția pe straturile derivate *U* și *V* este mult mai bună decât cea pe straturile lor de bază (*R* și respectiv *B*), astfel dimensiunea datelor auxiliare este redusă (tabelul 1). Stratul *G* este procesat separat folosind doar predicție de pe acest strat, aici se obțin rezultate similare cu metodele clasice).

Metoda VRBE prin substituție de MSB pentru fișiere audio folosește o serie de predictori anti-cauzali cu un context de predicție ce folosește 10-20 de eșantioane vecine.

Tabel 1. Numărul de pixeli cu valoarea MSB detectată greșit (predicție MED)

Imagine de test	**R+G+B**	**U+V+G**	**Imagine de test**	**R+G+B**	**U+V+G**
Kodim01	2007	737	*Kodim13*	25569	8534
Kodim02	638	248	*Kodim14*	3923	1473
Kodim03	625	248	*Kodim15*	1163	428
Kodim04	674	239	*Kodim16*	336	125
Kodim05	11909	4289	*Kodim17*	2795	1027
Kodim06	2862	954	*Kodim18*	7516	2693
Kodim07	1222	442	*Kodim19*	1596	604
Kodim08	9130	3134	*Kodim20*	2908	999
Kodim09	981	371	*Kodim21*	3291	1162
Kodim10	1739	565	*Kodim22*	1622	575
Kodim11	3874	1340	*Kodim23*	1269	425
Kodim12	745	263	*Kodim24*	15460	5220
			Medie pe set	**4328**	**1504**

În etapa II s-a optimizat și **metoda de inserție în imagini în clar cu menținere a histogramei erorii de predicție.** Menținerea după inserție a formei histogramei erorii de predicție permite un grad mai mare de securitate a datelor ascunse. Algoritmul propus determină parametrii de inserție ce mențin forma histogramei, dar care și limitează distorsiunea de inserție.

3. Dezvoltarea algoritm general de inserție reversibilă de date în domeniul criptat

Ultimul obiectiv principal, dezvoltarea unui algoritm general care să ofere avantajele ambelor abordări (VRAE și VRBE) nu a putut fi îndeplinit. Preprocesare folosită de VRBE permite folosirea unui algoritm de inserție ce introduce o distorsiune similară cu cea de la metodele pe imagini în clar. În schimb, metodele VRAE trebuie să asigure o inserție corectă a datelor indiferent de distribuția pixelilor în imaginea gazdă. Astfel, VRAE implică o inserția redundantă cu o distorsiune puternică asupra gazdei. Optimizările pentru VRAE reduc distorsiunea, însă nu suficient cât să fie comparativă cu cea de la VRBE. Cea mai performantă metodă VRAE oferă rezultate slabe comparativ cu o metodă VRBE relativ depășită. Bineînțeles, VRAE are avantajele sale: algoritmii de criptare și decriptare sunt standard, nu se transmit informații suplimentare despre gazdă. Metodele hibride investigate ajung să aibă nevoie de o preprocesare a oferii o performanță similară cu VRBE. Odată ce s-a folosit o preprocesare, metoda hibridă a devenit practic una pur VRBE.

În etapa III a proiectului s-a implementat și versiunea finală a metodei de **inserție reversibilă de capacitate mare în imagini.** Metoda aduce mai multe îmbunătățiri algoritmului standard PEE: optimizarea direcției de deplasare la ecuația de inserție, determinarea adaptivă a capacității inserate în fiecare pixel și implementarea unei codări rapide a datelor ascunse.

Algoritmul de optimizare a direcției de deplasare folosește valoarea prezisă și semnul erorii de predicție pentru a determina dacă biții ascunși sunt adunați sau scăzuți la inserție. Valoarea pixelului curent este modificată astfel încât să se depărteze de valoarea prezisă (pentru a crește eroarea de predicție). Ecuațiile de inserție nu schimbă semnul erorii de predicție, astfel direcția de deplasare este aleasă ca cea cu riscul cel mai mic de depășire. Această optimizare aduce un mic câștig pe majoritatea imaginilor (figura 2.a-b), însă poate aduce o creștere imensă în capacitate când avem un număr mare de pixeli cu valori la extreme (pur alb sau pur negru) cum se întâmplă la *Kodim20*, unde această optimizare aduce

o creștere în capacitate de 3 bpp. Această imagine are o regiune mare complet albă, pixelii din acea zonă au valoarea 255 și eroarea de predicție 0. La inserția clasică pixelii aceștia sunt cu risc maxim de depășire (informația secretă este adunată la tonul de gri), însă inserția propusă permite deplasarea în acest caz în direcția inversă (spre negru). Astfel, pixelii ce înainte nu puteau oferii capacitate sunt folosiți la o inserție multi-bit.

S-a investigat și efectul complexității predictorului asupra capacității maxime (figura 3. c-d). Folosirea unui predictor liniar, EGP, calculat pentru fiecare pixel pe baza unui bloc de învățare a dus la o creștere în capacitate de aproximativ 0,1 bpp.

Contribuția cea mai semnificativă adusă de această metodă este determinarea adaptivă a capacității de inserare în fiecare pixel. Se folosește valoarea prezisă și semnul erorii de predicție pentru a aproxima distanța dintre valoarea pixelului curent și extrema către care este deplasat (0, negru sau 255, alb). Un pixel este distorsionat maxim cu $(n-1)\cdot t$, unde *n* este numărul de biți ce se doresc a fi inserați și *t* este pragul de inserția. Pragul de inserție este stabilit în funcție de capacitatea dorită. Capacitatea maximă n_{max} poate fi estimată prin împărțirea diferenței față de extremă la pragul *t*. Această estimare este corectă cât timp eroarea de predicție curentă este mai mică decât pragul de inserție. Altfel inserția va produce o depășire, pentru acest caz se folosește o hartă de depășiri care este compresată și inserată într-o zonă rezervată a imaginii.

Avantajul principal al metodei, selectarea adaptivă a lui *n* la nivel de pixel introduce însă și o problemă de codare. Informația ascunsă este reprezentată de un șir binar necompresabil. Inserția prin PEE permite ascunderea de date și pentru valori a le lui *n* care nu sunt puteri a le lui 2. Soluția clasică este de a coda informația pe un număr de *n* simboluri, obținându-se o capacitate de $log_2 n$ biți. La metoda propusă valorile lui *n* variază de la un pixel la altul. O astfel de codare devine problematică: se determină numărul de pixeli inserați cu fiecare *n,* șirul de biți este spart în grupe, fiecare grupa este codată cu o valoare a lui *n* astfel încât să se obțină distribuțiile pe numărul de pixeli. Această problemă este întâlnită și la metoda din [9], însă acolo numărul de *n*-uri distincte este relativ mic (între 3 și 6).

Soluția la problema de mai sus este folosirea unei codări rapide sub-optimale, care permite inserția directă a datelor sub forma lor binară. Valoarea calculată *n* este rotunjită în jos la cea mai apropiată valoare ce permite folosirea directă a biților (folosindu-se un pas de cuantizare prestabilit).

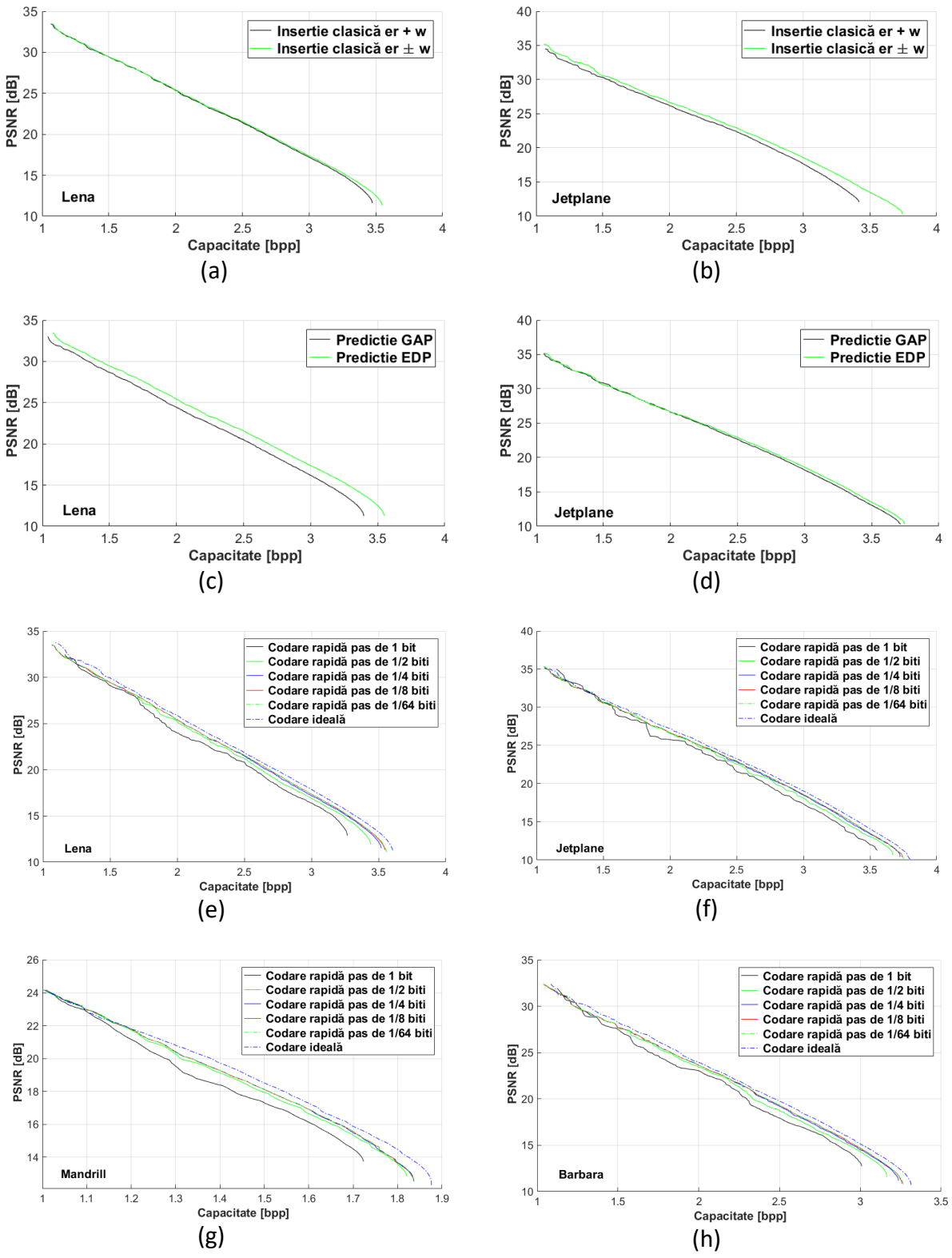

Figura 3. Rezultate metodă multi-bit propusă: optimizarea direcție de deplasare la inserție (a și b), predicția GAP și cea EDP (c și d), codările testate (e, f, g și h).

Pentru pașii de cuantizare mai mici de 1 bit, numărul de biți inserați variază în funcție de distribuția mesajului (aceste valori oferă o capacitate medie fixă, calculată pe baza probabilității de apariție a fiecărui caz). Figura 3. e-h prezintă efectul pasului de cuantizare asupra eficienței algoritmului propus. Se observă că pasul de cuantizare de 1/8 = 0,125 biți oferă rezultate echivalente cu pași mai mici, astfel aceasta reprezintă pasul ideal de cuantizare pentru codarea și inserția rapidă a mesajului secret. Este important de precizat că dicționarul de codare nu depinde de mesajul curent, aceasta are o formă fixă care nu depinde de imaginea gazdă, astfel nu este nevoie ca acesta să fie stocat.

Tabel 2. Îmbunătățirile în capacitate oferite de metoda propusă

Imagine de test	**Capacitate raportată în [9]**	**Capacitate metodă propusă [bpp]**			**Imagine de test**	**Capacitate raportată în [9]**	**Capacitate metodă propusă [bpp]**		
		GAP, codare rapidă	**EDP, codare rapidă**	**EDP, codare ideală**			**GAP, codare rapidă**	**EDP, codare rapidă**	**EDP, codare ideală**
Kodim01	2.140	2,338	2,377	2,414	*Kodim13*	1.389	1,653	1,686	1,719
Kodim02	3.381	3,569	3,629	3,676	*Kodim14*	2.421	2,634	2,718	2,758
Kodim03	4.028	4,055	4,324	4,386	*Kodim15*	2.605	3,510	3,613	3,652
Kodim04	3.294	3,437	3,542	3,595	*Kodim16*	3.254	3,378	3,526	3,575
Kodim05	2.208	2,367	2,509	2,547	*Kodim17*	2.952	3,288	3,421	3,480
Kodim06	2.365	2,910	3,019	3,058	*Kodim18*	2.183	2,466	2,541	2,578
Kodim07	3.864	3,884	4,043	4,108	*Kodim19*	2.959	3,105	3,190	3,243
Kodim08	1.888	2,180	2,173	2,210	*Kodim20*	1.177	4,125	3,986	4,042
Kodim09	3.556	3,643	3,793	3,859	*Kodim21*	2.884	3,079	3,121	3,169
Kodim10	3.532	3,668	3,770	3,839	*Kodim22*	2.928	3,106	3,158	3,206
Kodim11	2.765	3,063	3,133	3,174	*Kodim23*	3.911	4,113	4,271	4,341
Kodim12	3.188	3,663	3,792	3,843	*Kodim24*	2.552	3,045	2,990	3,034
					Medie pe set	**2.809**	**3,178**	**3,263**	**3,313**

Metoda propusă oferă cele mai mari capacități de inserție raportate până acum (tabelul 2), depășind rezultatele oferite de [8] și [9] pe toate imaginile testate.

Articolul pentru inserție reversibilă de capacitate mare este în curs de submitere la *IEEE Trans. on Information Forensics and Security.* Algoritmul de codarea rapidă (o parte cheie a metodei propuse) a fost implementat în etapa III.

Această metodă pentru imagini în clar poate fi adaptată pentru domeniul criptat. Pentru a menține reversibilitatea se folosește un prag de cuantizare de 1 bit. Algoritmul de inserție în domeniul criptat este unul derivat din inserția reversibilă prin substituție de LSB: se determină valorile distincte ale lui *n* care se poate memora o hartă de poziții. Se aplică o permutare pe blocuri pentru a nu permite identificare imaginii gazdă din harta de poziții. În etapa de preprocesare se efectuează deplasarea pixelilor pentru eliberarea pozițiilor ocupa ce vor fi ocupate de datele ascunse. După criptare, harta este citită din zona rezervată, iar pe baza ei se distribuie adaptiv mesajul secret în pixelii indicați de hartă.

Rezultate semnificative ale cercetărilor

Rezultatele din cadrul proiectului CREED s-au concretizat printr-o serie de noi metode de inserție reversibilă a datelor în imagini digitale (criptate și în clar, metodele în clar având și un echivalent în domeniul criptat) și fișiere audio criptate. Principalele rezultate sunt următoarele:

- Două metode de inserție reversibilă în domeniu criptat prin VRAE. Prima metodă este bazată pe un nou set de predictori pentru detecția datelor cu predictori multipli. A doua metodă are la bază predicția în ordine raster-scan pe blocuri disjuncte și pe gruparea aleatoare a pixelilor gazdă.
- Trei metode de inserție reversibilă în domeniu criptat prin VRBE. Prima metodă este derivată din cea VRAE bazată pe blocuri. A doua abordare are introduce un nou set de ecuații ce permite inserția reversibilă prin substituție de LSB. Iar ultima abordare adaptează inserția în MSB introdusă în [5] pentru imagini color și fișiere audio.
- O nouă metodă de inserție reversibilă în imagini prin PVO bazată pe o parcurgere șir vectorial a pixelilor gazdă.
- Un nou algoritm de inserție reversibilă ce menține forma histogramei erorii de predicție.

- O nouă metodă de inserție reversibilă de capacitate mare în imagini care a crescut limita de inserție în imagini cu 0,4-0,5 bpp. Capacitatea maximă pe setul Kodak a crescut de la 2,8 bpp la 3,3 bpp, obținându-se pe unele imagini de test capacități de 4 bpp (pe imagini cu tonuri de gri pe 8 biți).

Din păcate rezultatele prezentate mai sus nu s-au materializat ca articole în timp util. Pandemia de COVID a făcut deplasarea la conferințe imposibilă. Rezultatele obținute inițial de algoritmii propuși au fost insuficiente pentru susținerea lor, optimizările ulterioare permit publicarea lor, însă timpul rămas nu a mai permis acest lucru. Îmbunătățirile aduse metodei PVO sunt de interes, însă versiunea curentă a articolului folosește o versiune PVO recent depășit. Optimizarea găsită se poate aplica noi metode. Menționăm însă ca noile metode PVO din domeniu sunt mult mai complexe decât abordările clasice. Acestea determină adaptiv setul de ecuații de inserție în funcție de distribuția histogramei 2D a erorii de predicție, algoritmii clasici PVO (pe care s-a realizat metoda propusă) folosesc un set de ecuații predefinit. Metoda de inserție de capacitate mare crește performanțele în domeniul inserției reversibile. Articolul este în curs de submitere la *IEEE Trans. on Information Forensics and Security,* o revistă roșie (în topul 25% al jurnalelor de specialitate). Metoda a fost schițată în prima etapă a proiectului, însă optimizările ce permit publicarea sa la nivelul dorit au fost găsite în etapa III.

Rezultatele estimate la începutul proiectului de 2-3 articole de revistă roșie nu au fost realizate datorită atât domeniului competitiv al inserției în imagini, precum și plafonarea rezultatelor pentru inserția în domeniul criptat. Metode suficient de performante pentru astfel de publicații au fost găsite (inserția reversibilă de capacitate mare, VRBE cu permutarea blocurilor și noua abordare PVO), însă nu s-a reușit publicare lor în perioada proiectului.

Concluzii

Rezultatele obținute în cadrul CREED au dus la creșterea performanțelor în domeniul inserției reversibile. Echipa a îmbunătățit unele metode existente (VRAE în pixeli selectați aleator, inserția generală VRBE, metoda PVO) și a venit cu noi abordări (noi ecuații ce permit inserția reversibilă prin substituție de LSB, inserția adaptivă a biților ascunși în funcție de valoarea prezisă, inserția reversibilă ce menține histograma erorii de predicție).

Performanțele obținute la inserția în domeniul criptat au fost limitate (o singură metodă VRBE ce poate fi publicată la un jurnal în topul 25%), însă s-au descoperit îmbunătățiri relevante pentru inserția reversibilă clasică în imagini, un domeniu mult mai competitiv.

Director Proiect,

S.L.dr.ing. Ioan Cătălin DRĂGOI

Bibliografie

[1] X. Wu, W. Sun „High-capacity reversible data hiding in encrypted images by prediction error”, Signal Processing, pp. 387–400, 2014.

[2] I.C. Dragoi, D. Coltuc „Reversible data hiding in encrypted images based on reserving room after encryption and multiple predictors”, IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2018.

[3] I.C. Dragoi, D. Coltuc, I. Caciula „Gradient based prediction for reversible watermarking by difference expansion”, Proceedings of the 2nd ACM workshop on Information hiding and multimedia security, 2014.

[4] D. Xiao, et al. „Separable reversible data hiding in encrypted image based on pixel value ordering and additive homomorphism”, Journal of Visual Comm. and Image Representation 45: 1-10, 2017.

[5] P. Puteaux and W. Puech, ”An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images”, IEEE Trans. Inf. Forensics Security, 7, pp. 1670-1681, 2018.

[6] Kaur, Gurjinder, et al. "A comprehensive study of reversible data hiding (RDH) schemes based on pixel value ordering (PVO)." *Archives of Computational Methods in Engineering* 28.5 (2021): 3517-3568.

[7] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, ”High capacity reversible data hiding in encrypted images by patch-level sparse representation”, IEEE Trans. Cybernetics, vol. 46, pp. 1132–1143, 2016.

[8] Huang, H. C., Chang, F. C., & Lu, Y. Y. (2017). Multi-Bit Reversible Data Hiding with Prediction and Difference Alteration. *J. Inf. Hiding Multim. Signal Process.*, *8*(2), 435-444.

[9] Caciula, I., Coanda, H. G., & Coltuc, D. (2019). Multiple moduli prediction error expansion reversible data hiding. *Signal Processing: Image Communication*, *71*, 120-127.