

## RAPORT

### ETAPA I: Algoritmi marcare reversibilă de mare capacitate

Eforturile echipei de cercetare în această etapă s-au concentrat asupra dezvoltării algoritmilor de marcare reversibilă de mare capacitate atât în domeniul spațial, cât și în domeniul criptat. Obiectivele proiectului au fost îndeplinite. În acest sens, menționăm elaborarea a 5 familii de algoritmi noi cu performanțe îmbunătățite față de algoritmi cunoscuți.

**Activitatea 1.1. Management și diseminare.** Directorul de proiect a asigurat coordonarea activităților având grijă de sincronizare și a supervizat activitatea de diseminare. Astfel, cercetările din aceasta etapă au fost diseminate prin următoarele publicații:

- 1) I.-C. Dragoi, H.-G. Coanda, D. Coltuc, "Improved Reversible Data Hiding in Encrypted Images Based on Reserving Room After Encryption and Pixel Prediction", *25th European Signal Processing Conference (EUSIPCO)*, vol. 23, no. 4, p. 2250-2254, Kos, Grecia, 2017.
- 2) I.-C. Dragoi, D. Coltuc, H.-G. Coanda "Adaptive pairwise reversible watermarking with horizontal grouping," *IEEE International Symposium on Signals, Circuits and Systems (ISSCS)*, Iasi, Romania, 2017.
- 3) I.-C. Dragoi, D. Coltuc, "Reversible Data Hiding in Encrypted Images Based on Reserving Room After Encryption and Multiple Predictors," in curs de revizie la *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, 2018.

Două articole sunt în fază finală de redactare și urmează a fi trimise spre evaluare și publicare la revistele *IEEE Transactions on Image Processing* și, respectiv, *IEEE Transactions on Information, Forensics and Security*:

- 4) I.-C. Dragoi, I. Caciula, D. Coltuc, "Pairwise Color Image Reversible Watermarking" in curs de submitere la *IEEE Transactions on Information, Forensics and Security*.

- 5) I.Caciula, D. Coltuc, “Multiple Moduli Prediction-Error Expansion Reversible Watermarking” in curs de submitere la *IEEE Transactions on Image Processing*.

Menționăm că ambele reviste sunt clasificate în Q1 (reviste roșii) cu factori de impact 4,828 și, 4,332.

De asemenea, tot în scopul diseminării rezultatelor cercetărilor, directorul de proiect împreună cu prof. William PUECH de la *Laboratoire d’Informatique, de Robotique et de Microelectronique de Montpellier, CNRS, Univ. Montpellier, France*, au propus organizarea unei sesiuni speciale cu profilul “*Data Hiding in the Encrypted Domain*” în cadrul conferinței *IEEE International Conference on Image Processing (ICIP) 2018*, conferință aflată la a 25-a ediție. Menționăm că, *IEEE ICIP* este conferința far din domeniul prelucrării imaginilor. La această sesiune specială, echipa UVT intenționează să participe și cu un articol cu titlul “*Reversible Data Hiding in Encrypted Images with Block Based Prediction*”, autori I.-C. Dragoi și D. Coltuc. Rezultate preliminare promițătoare au fost deja obținute, iar data pentru trimiterea articolului este 26.02.2018. Anunțarea rezultatelor cu privire la sesiunile speciale sunt așteptate pe data de 15.12.2017.

**Activitatea 1.2 : Analiza algoritmilor de capacitate mare publicați în literatură.** Au fost analizați algoritmi cu performanțele cele mai bune publicate în literatură atât pentru imagini cu nivele de gri, cât și pentru imagini criptate. Pentru imagini cu nivele de gri au fost analizați algoritmul lui X. Li et al., [1] și algoritmul lui X. Gui et al., [2]. Algoritmul [1] se dovedește a fi un caz particular al algoritmului [2]. Pentru inserție în perechi au fost analizați algoritmi [3,4] și algoritmul nostru propus în [5]. Pentru imagini criptate, domeniu dificil, dar în mare avânt datorită dezvoltării tehnologiilor tip « cloud », algoritmul [6], algoritmul de tipul VRAE (*vacating room after encryption*). Menționăm că algoritmi VRAE utilizează scheme de criptare standard, ceea ce asigură un nivel ridicat de securitate. Spre deosebire de algoritmi tip RRBE (*reserve room before encryption*), oferă capacități de inserție mai mici, de unde intreresele de a îmbunătăți capacitatea de inserție.

**Activitatea 1.3: Dezvoltarea de noi scheme de inserție multibit cu optimizarea modulului de expandare și compresie fără pierderi.** Schemele de marcare reversibilă de tip

PEE (PEE -*prediction error expansion*) bazate pe expandarea erorii de predicție oferă o capacitate de inserție mai mare datorită faptului că exploatează mai bine corelația dintre pixeli. Pentru atingerea de capacități mari de inserție se pot folosi scheme de tip PEE-MB (PEE multibit), unde eroarea de predicție este expandată de  $n$ -ori ( $n \geq 2$ ) pentru a insera  $\log_2 n$  biți pe pixel. Creșterea capacității de inserție în schemele PEE-MB se obține prin controlul parametrului  $n$ . Principiul schemei MB este de a expanda de  $n$ -ori eroarea de predicție pentru a putea insera marcajul în eroarea de predicție expandată. După ce eroarea de predicție este expandată de  $n$ -ori, putem insera marcajul printr-o operație de adunare. Valoarea pixelului marcat trebuie să fie în domeniul de reprezentare al imaginii:  $x' \in [0,255]$ . Pentru situațiile în care avem depășiri se folosește o hartă de poziții binară unde se va memora valoarea 1 pentru pixelii marcați și 0 pentru pixelii care nu pot fi marcați deoarece produc depășiri ( $x' \notin [0,255]$ ). În schema propusă vom analiza capacitatea maximă de inserție oferită de fiecare pixel. Fie  $m \geq 1$  modulul pixelului  $x$  dacă condiția următoare este respectată:

$$0 \leq x' = x + (m - 1)p_e + w \leq 255 \quad 1$$

Marcajul  $w$  ia valori întregi și aparține intervalului  $[0, m-1]$ . Fiecare pixel din imagine va avea asociat un modul maxim  $n$  cu care pixelul se poate marca folosind expandarea erorii de predicție. Modulul maxim  $n$  pentru pixelul original  $x$  este dat de următoarea relație:

$$n = \max\{m \mid 0 \leq x + (m - 1)p_e + w \leq 255\} \quad 2$$

Deoarece pentru fiecare pixel din imagine putem calcula modulul său maxim, vom construi o hartă de moduli  $M$  care va fi asociată imaginii. Harta de moduli va avea o semnificație diferită de harta de poziții clasică: ne va oferi capacitatea maximă de inserție dată de fiecare pixel din imagine. De exemplu, dacă pentru pixelii de pe poziția (1,1) din imagine originală avem modulul maxim  $n=2$  în harta de moduli, atunci capacitatea maximă de inserție a pixelului este:  $\log_2 2=1$  bit. Vom nota cu  $H$  histograma hărții de moduli. Folosind harta de moduli putem calcula limita superioară a capacității maxime de inserție  $C$  pentru schemele bazate pe expandarea erorii de predicție folosind relația de mai jos:

$$C = \frac{1}{P} \sum_{i=1} H(i) \log_2 i \text{ [bpp]} \quad 3$$

Relația de mai sus ne oferă capacitatea maximă pe care o putem insera în imaginea originală folosind harta de moduli. Observăm că această capacitate maximă este mai mare decât

cea obținută în cazul schemei multibit. După ce harta de moduli a fost compressată fără pierderi, ea va fi adăugată ca informație adițională. Informația adițională trebuie să ocupe un spațiu mai mic decât capacitatea de inserție oferită de metoda de marcarea. Dacă spațiul ocupat de informația adițională este mai mare decât capacitatea de inserție obținută prin folosirea hărții de moduli, atunci schema de marcarea nu este reversibilă. Pentru aceasta ne vom concentra pe reducerea spațiului ocupat de harta de moduli compressată. Pentru a crește rata de compresie a hărții de moduli, aceasta va fi compusă din  $k$  ( $k > 1$ ) moduli. Fie  $1 < n_1 < n_2 \dots n_k$  valorile celor  $k$  moduli. Vom nota cu  $M(n_1, n_2 \dots n_k)$  harta generată de utilizarea a  $k$  moduli. Harta de moduli  $M(n_1, n_2 \dots n_k)$  se va obține prin transformarea hărții originale de moduli  $M$ . Fie  $n$  modulul maxim al pixelului din harta de moduli  $M$ . Toți pixelii care au modulul  $n < n_j$  în harta  $M$  nu vor fi marcați. Pentru acești pixeli vom memora valoarea 1 în harta  $M(n_1, n_2 \dots n_k)$ . În cazul în care  $n \in [n_j, n_{j+1})$ , ( $\forall j = 1..k - 1$ ), vom memora valoarea  $n_j$  în harta  $M(n_1, n_2 \dots n_k)$ . În final, dacă  $n \geq n_k$ , atunci se va memora valoarea  $n_k$  în harta  $M(n_1, n_2 \dots n_k)$ . Vom maximiza următoarea funcție de calcul  $C(n_1, n_2 \dots n_k)$  a capacității de inserție:

$$\frac{1}{P} \sum_{j=0}^k \sum_{i=n_j}^{n_{j+1}-1} H(i) \log_2(n_j) - \left( -\frac{1}{P} \sum_{j=0}^k \left( \sum_{i=n_j}^{n_{j+1}-1} H(i) \right) \log_2 \frac{1}{P} \left( \sum_{i=n_j}^{n_{j+1}-1} H(i) \right) \right) \text{ [biți]} \quad 4$$

Pentru a atinge capacitatea maximă de inserție trebuie să determinăm următorii parametri:  $k$  și mulțimea de moduli  $(n_1, n_2 \dots n_k)$ , care maximizează relația de mai sus. Deoarece funcția de mai sus nu poate fi maximizată direct folosind metoda programării lineare, vom construi doua matrici: matrice de cost  $W$  și matrice de validare  $Y$  de dimensiune  $(N + 1) \times (N + 1)$  fiecare. Observăm că capacitatea obținută prin alegerea modului  $n_j$  depinde de modulul superior  $n_{j+1}$ . Elementele matricei de cost  $W$  ne oferă informații despre capacitatea oferită de alegerea modului  $i$  atunci când modulul superior  $j$  variază. Termenul  $w_{ij}$  al matricei  $W$  este definit astfel :

$$w_{i,j} = \begin{cases} \left( \sum_{t=i}^{j-1} \frac{H(t)}{P} \right) \log_2 i - \left( \sum_{t=i}^{j-1} \frac{H(t)}{P} \right) \log_2 \left( \sum_{t=i}^{j-1} \frac{H(t)}{P} \right), & \text{dacă } i < j \\ 0, & \text{altfel} \end{cases} \quad 5$$

Vom extinde soluția cu  $k$  moduli  $n_1, n_2, \dots, n_k$  cu termenii  $n_0=1$  și  $n_{k+1}=N+1$ . Modulul  $n_0=1$  este util pentru calculul entropiei pixelilor care nu se transformă, iar modulul  $n_{k+1}$  este util în evaluarea contribuției în capacitate a modulului  $n_k$ . Deoarece termenii soluției  $n_0 < n_1 < \dots < n_{k+1}$  sunt în ordine strict crescătoare, vom folosi matricea de validare binară  $Y$  pentru a impune relația de strictă ordine și existență a modurilor în procesul de căutare a soluției. Termenul  $y_{i,j}$  al matricei  $Y$  este definit după cum urmează:

$$y_{i,j} = \begin{cases} 1, & \text{dacă } i < j < N + 1 \text{ și } H(i)H(j) \neq 0 \\ 1, & \text{dacă } i < j = N + 1 \text{ și } H(i) \neq 0 \\ 0, & \text{altfel} \end{cases} \quad 6$$

Valorile de 1 în matricea  $Y$  asigură că perechea de modulul  $i$  și  $j$  pot face parte din soluția finală. Vom asigura existența modulului  $n$  în harta de moduli prin impunerea condiției  $H(n) \neq 0$ . Fie mulțimea de întregi  $X=1,2,\dots,N+1$  și  $S \subseteq X$  soluția extinsă cu  $S(1)=1, S(k+2)=N+1$ . Capacitatea dată de soluția  $S$  folosind matricea de cost  $W$  și matricea de validare  $Y$  este următoarea:

$$C_k(S) = \sum_{i=1}^{k+1} w(S(i), S(i+1)) \cdot y_{S(i), S(i+1)} \text{ [bpp]} \quad 7$$

Capacitatea maximă de inserție depinde de găsirea combinațiilor valide de moduli  $(S(i), S(i+1))$ . Folosind programarea lineară putem maximiza funcția  $C_k(S)$ . Pentru aceasta vom introduce matricea binară de decizie  $Z$  prin care vom reprezenta soluția problemei. Dimensiunea matricei  $Z$  este  $(N+1) \times (N+1)$  și termenul  $z_{i,j}=1$  dacă modulii  $i$  și  $j$  sunt doi moduli consecutivi în soluția  $S$ . Funcția de optimizat folosind modelul de programare lineară propus este următoarea:

$$\max \sum_{i=1}^{N+1} \sum_{j=1}^{N+1} z_{i,j} \cdot w_{i,j} \text{ [bpp]} \quad 8$$

Modelul propus mai sus este independent de predictor. În cazul predictorilor GAP[11], respectiv EDP[12]. Pentru imaginea standard Lena se depășește pentru prima dată pragul de 3 bpp: 3.07 bpp (GAP), respectiv 3.22 bpp (EDP). În comparație cu cea mai bună schemă de marcarea de mare capacitate propusă de Gui ș.a în [2], metoda propusă aduce un câștig mediu de 0.1-0.3 bpp. Pentru setul standard de imagini (*lena, mandrill, tiffany, jetplane, barbara, boat, house* și *lake*) în cazul predictorul GAP câștigul mediu este de 0.1475 bpp, respectiv 0.3604 bpp. Pe setul extins de imagini Kodak (24 de imagini), câștigul mediu este de peste 0.3 bpp. Cea mai mare rată de inserție este obținută pentru imaginea *kodim3*: 4.019 bpp (folosind predictorul EDP). De notat

faptul că timpul de execuție pentru metoda propusă este de câteva secunde pentru determinarea parametrilor de marcare în comparație cu metoda lui Gui ș.a care are un timp de execuție de cel puțin 1 minut datorită căutării soluție folosind metoda brute-force. Un articol asupra marcării multibit cu module multiple urmează a fi trimis pentru publicare la *IEEE TIP*.

#### **Activitatea 1.4: Dezvoltarea de scheme multibit cu estimarea hărții modulelor de expandare.**

Au fost întreprinse cercetări pentru reducerea dimensiunii hărții modulelor și, implicit pentru creșterea capacității de inserție a algoritmilor tip multimodul de expandare. Cercetările sunt promițătoare și vor fi continuate în etapa următoare. De asemenea, au fost întreprinse cercetări pentru îmbunătățirea capacității de inserție pentru imagini criptate. Astfel, menționăm elaborarea a doi algoritmi originali cu performanțe îmbunătățite față de algoritmi cunoscuți. Metodele de marcare pentru imagini criptate sunt clasificate în două categorii distincte în funcție de cum creează spațiul necesar pentru stocarea mesajului ascuns. Prima categorie, cunoscută în literatură ca „*reserving room before encryption*” (RRBE) cuprinde metodele care efectuează o etapă de preprocesare a imaginii înainte ca aceasta să fie criptată. Metode RRBE oferă capacități mari de inserție și distorsiuni mici de marcare (raportul capacitate/distorsiune oferit este similar cu cel obținut de metodele de marcarea reversibilă din domeniul necriptat). Însă algoritmi RRBE au și o serie de slăbiciuni, cele mai semnificative fiind legate de securitatea criptării. A doua categorie de metode este „*vacating room after encryption*” (VRAE). Aceste metode lucrează direct pe imaginea criptată, metoda de criptare este una clasică din domeniu (de obicei se folosește criptarea pe bază de SAU exclusiv), iar corelația dintre pixeli este exploatată doar la extragerea marcajului. Citirea și extragerea marcajului trebuie să fie realizabilă indiferent de conținutul imaginii, astfel distorsiunile de inserție sunt mari (pentru a garanta că modificările făcute sunt detectabile indiferent de complexitatea imaginii), iar capacitatea de inserție este mică (un bit de informație este inserat într-un grup de pixeli pentru a garanta citirea lui corectă). Însă metodele VRAE rămân mai practice decât cele RRBE deoarece nu au nevoie de preprocesare și nu depind de o metodă proprie pentru criptare.

Primul algoritm pentru imagini criptate propus pornește de la schema lui Wu și Sun, [6] și aduce ca noutăți două etape de inserție/decodare și o procedură de inserție bazată pe paritate. La fel ca la schema originală putem evidenția două moduri distincte de funcționare. În modul 1 se efectuează citirea și extragerea marcajului după ce imaginea a fost decriptată, extragerea

aducând pixelii gazdă la valoarea lor inițială. În modul doi se face citirea și rescrierea marcajului fără să fie nevoie de decriptare (sacrificând citirea după decriptare), însă restaurarea imaginii gazdă se face pe versiunea decriptată. Inserția bazată pe paritate introdusă în schema propusă reduce semnificativ nevoia de a distorsiona straturile de biți apropiate de MSB (*Most Significant Bit*) la metoda de marcarea II, eliminându-se astfel principalul dezavantaj al schemei propuse de Wu și Sun: aspectul zgomotos al imaginii decriptate după marcarea. Compromisul făcut de Wu și Sun pentru eliminarea zgomotului (folosirea unui filtru median) nu mai este necesar. Fata de algoritmi publicați până acum pentru marcarea în imagini criptate, schema noastră oferă capacitate de inserție mai mare la distorsiuni mai mici. Câștigul în capacitate este datorat celor două etape de inserție/decodare. Schemele de marcarea în imagini criptate din literatură împart pixelii din imagine în două seturi distincte: setul gazdă ce conține marcajul și setul de referință, care este folosit la citirea/extragerea marcajului (metoda I) sau la restaurarea imaginii (metoda II). La aceste scheme s-a considerat că pixelii ce aparțin setului de referință (jumătate din imagine) nu pot fi modificați, astfel ei nu pot conține biți ascunși, limitând capacitatea oferită de schemă. Cele două etape de inserție/decodare permit introducerea unui al treilea set de pixeli. Acesta este marcat, iar la decodare poate fi folosit ca referință pentru setul inițial de pixeli gazdă. După ce noul set este restaurat, acesta este folosit împreună cu setul de referință pentru a extrage mesajul/restaura setul gazdă principal (jumătate din imagine). În concluzie, numărul maxim de pixeli ce pot fi folosiți la marcarea crește de la jumătate la trei sferturi din imagine. Algoritmul a fost prezentat la EUSIPCO 2017.

Al doilea algoritm este tot de tip VRAE și are la bază metoda propusă de noi la conferința EUSIPCO. Schemele de marcarea din acest domeniu, inclusiv metoda noastră precedentă, folosesc o singură formulă (de obicei un predictor) pentru a determina bitul inserat într-un grup de pixeli. Algoritmul propus alege adaptiv pentru fiecare grup de pixeli unul sau mai mulți predictorii pe un context de predicție prestabilit. Acești predictorii sunt media aritmetică, media ponderată pe bază de gradienti, medianul și estimarea *midpoint* (media dintre valoarea minimă și cea maximă). Selecția se realizează pe baza gradului de încredere atribuit fiecărui predictor pentru grupul curent de pixeli. Toți pixelii dintr-un grup sunt originali dacă bitul inserat a fost „0” sau sunt distorsionați cu  $\pm 2T$  dacă bitul inserat a fost „1” (stratul de biți  $T$  fiind ales pentru marcarea), astfel un predictor care a detectat cu aceeași probabilitate ambele cazuri într-un singur

grup nu a obținut rezultate de încredere. Aceste rezultate sunt excluse, algoritmul ghidându-se numai după rezultatele care favorizează un anumit caz.

Marcarea se face în două etape, idee preluată din metoda precedentă, însă acum parametrii de inserție variază în funcție de etapa curentă. Etapa I folosește un context de predicție format din vecinii diagonali ai pixelilor gazdă. Acest context este mai dificil decât cel folosit în etapa II (cei mai apropiați vecini orizontali/verticali). Astfel grupele din prima etapa de marcarea vor conține un număr mai mare de pixeli pentru a compensa efectul negativ avut de context asupra predicției. Rezultatele experimentale indică că noua metodă aduce un câștig în PSNR care ajunge la 5 dB față de metoda noastră precedentă și cea a lui Wu et al. . Se observă și o creștere în capacitate de până la 0.05 bpp față de metoda precedentă și 0.1 bpp față de Wu [6]. Un articol care descrie algoritmul propus este în curs de evaluare la IEEE ICASSP 2018.

**Activitatea 1.5: Dezvoltarea de mecanisme de control al distorsiunii pentru inserție multibit.** Pentru reducerea distorsiunilor algoritmilor de marcarea am investigat problema controlului fin al inserției precum și elaborarea unor scheme originale de inserție. Ca rezultate principale menționăm doi algoritmi originali.

Primul algoritm pleacă de la algoritmul de inserție cu împerechere adaptivă publicat în [5] și schimbă procedura de împerechere prin favorizarea grupării în direcție orizontală. Gruparea orizontală impune o nouă schemă de predicție, o procedură de măsurare a complexității ușor diferită, o nouă procedură de selectare a pixelilor și alte câteva mici ajustări. Reamintim că metoda originală din *IEEE TIP* 2016 împarte imaginea în două submulțimi disjuncte (ca patratelele unei table de sah) și împerechează pixeli aparținând unei submulțimi, iar cealaltă submulțime se folosește la predicție. Aspectul inovativ introdus de noua schemă este utilizarea vecinilor orizontali apropiați, la constituirea perechilor. Bineînțeles, vecinii orizontali adiacenți nu mai pot participa la predicția pixelului curent. În această situație, am dezvoltat un nou predictor care utilizează vecinii de pe liniile care încadrează pixelul curent. Predictorul a fost verificat prin testare intensivă pe seturile standard de imagini folosite în marcarea reversibilă. Am dezvoltat și o nouă măsură pentru complexitatea contextului, măsură care se dovedește mai eficientă decât cea utilizată în metoda originală. Schema propusă poate depăși schema noastră adaptivă publicată în 2016, schemă care are performanțele cele mai bune raportate până în prezent în literatură pentru inserție cu distorsiuni reduse. precum și alte 2

scheme foarte performante din aceeasi categorii, respectiv [9,10]. Dependența performanțelor de imaginea gazdă poate fi rezolvată, și anume, se calculează inițial histograma erorilor de predicție pentru predictorul medie aritmetică pe V4 (folosit de schema din 2016) și medie aritmetică ponderată pentru noua schemă și se alege schema pentru care se estimează performanțele cele mai bune, respectiv eroarea de predicție cea mai mică. Algoritmul a fost prezentat la IEEE ISSCS 2017, conferință indexată ISI Proceedings.

Al doilea algoritm extinde inserția adaptivă în perechi la imagini color. Articolele publicate pe domeniul marcării reversibile a imaginilor color urmăresc inserția eficientă a mesajului ascuns. Valorile din fiecare plan de culoare sunt distorsionate de marcarea cu cel mult  $\pm 1$ , astfel eroarea pătrată maximă inserată într-o valoare este 1. Metodele curente din literatură tind să ignore corelația dintre planele de culoare (Ou et al., [13]) sau să se folosească de ea indiferent de statistica individuală a imaginii curente (Yao et al., [14]). Noi propunem alegerea planelor de culoare folosite pentru marcarea în funcție de statistica imaginii curente. Pe lângă planele RGB se determină și trei plane derivate:  $U=R-G$ ,  $V=B-G$  și  $W=R-B$ . Pentru fiecare plan se calculează eroarea de predicție a pixelilor pe baza mediei aritmetice pe contextul romb (cei mai apropiați vecini orizontali și verticali). Se calculează apoi valoarea  $sk$ , aceasta reprezintă numărul de pixeli cu cele mai reprezentate erori din histograma fiecărui plan. Valorile  $sk$  sunt apoi sortate în ordine descrescătoare. Cele trei plane de culoare cu valorile  $sk$  cele mai mari vor fi folosite la marcarea. Planele derivate ( $U$ ,  $V$  și  $W$ ) sunt marcate prin modificarea planelor clasice corespunzătoare lor. Dacă o valoare din planul  $R$  este modificată:  $x=x+1$ , atunci valoarea corespunzătoare din  $U=R-G$  devine  $y=y+1$ . În mod similar, dacă o valoare din  $B$  a fost modificată:  $x=x+1$ , atunci valoarea corespunzătoare din  $W=R-B$  devine  $y=y-1$ . Algoritmul de marcarea pe bază de perechi de pixeli este și el adaptat pentru inserția în imagini color. Planele selectate pot permite (în funcție de cazul curent) marcarea simultană în două dintre ele. Dacă două erori de predicție pot fi calculate simultan, atunci acestea pot fi grupate în perechi. Algoritmul de creare a perechilor consideră acum ca o posibilă pereche pentru un pixel și valoarea de pe aceeași poziție dintr-un plan ce poate fi marcat simultan cu cel curent. Astfel se exploatează corelația dintre plane pentru a produce perechi ce permit o marcarea eficientă (care poate fi realizată doar când erorile din pereche au valori similare). Comparativ cu cea mai performantă metodă din literatură, [14], algoritmul propus oferă un câștig mediu de aproximativ 0.75 dB pe setul Kodak la o capacitate de 50 000 biți. Metoda noastră este și mai puțin complexă

comparativ cu predicția liniară (și filtrarea) folosită de Yao et al. Un articol care descrie algoritmul urmează să fie submis în decembrie 2017 la *IEEE Transactions on Information Forensics and Security*.

**Activitatea 1.6: Implementare algoritmi marcarea reversibilă.** Au fost implementați (MatLab) algoritmi analizați în A1.2, anume algoritmi descriși în [1]-[4]. Singurul algoritm care a ridicat dificultăți de implementare a fost algoritmul [2], din cauza complexității ridicate a calculului pentru etapele de determinare prin căutare exhaustivă a parametrilor. Evident, pentru algoritmul [5], algoritm propus de doi membri ai echipei proiectului, codul MatLab era deja disponibil în cadrul echipei UVT. Au fost implementate și o serie de variante ale algoritmilor originali propuși în A1.3 - A1.5.

**Activitatea 1.7: Testare algoritmi marcarea reversibilă.** Au fost definite protocoale de testare atât pentru imaginile în clar, cât și pentru imaginile criptate și au fost testați intensiv algoritmi descriși în [1-4]. S-a verificat pentru algoritmi [1-4] obținerea rezultatelor publicate de autorii lor. Au fost testați algoritmi originali propuși și au fost validate variantele cu performanțele cele mai bune. Variantele selectate au fost comparate cu algoritmi [1-4].

**Activitatea 1.8: Achiziție echipamente și materiale.** Achizițiile s-au desfășurat conform prevederilor contractului și anume, server, calculatoare, imprimante, kituri FPGA, publicații și acces IEEE, diverse materiale (hârtie, toner) samd.

## **Bibliografie**

1. X. Li, B. Yang and T. Zeng, "Efficient Reversible Watermarking Based on Adaptive Prediction-Error Expansion and Pixel Selection", *IEEE Trans. on Image Process.*, vol. 20, no. 12, pp. 3524–3533, 2011.
2. X. Gui, X. Li and B. Yang, "A High Capacity Reversible Data Hiding Scheme Based on Generalized Prediction-Error Expansion and Adaptive Embedding", *Signal Process.*, vol. 98, pp. 370-380, 2014.

3. B. Ou, X. Li, Y. Zhao, R. Ni and Y.-Q. Shi, "Pairwise Prediction-Error Expansion for Efficient Reversible Data Hiding," *IEEE Trans. on Image Processing*, vol. 22, no. 12, pp. 5010–5021, 2013.
4. S. Cai, X. Li, J. Liu and Z. Guo, "A new reversible data hiding scheme exploiting high-dimensional prediction-error histogram," *IEEE Intl. Conf. on Image Processing (ICIP)*, pp. 2732–2736, 2016
5. I.-C. Dragoi and D. Coltuc, "Adaptive pairing reversible watermarking," *IEEE Trans. Image Process.*, vol. 25, no. 5, pp. 2420–2422, 2016.
6. X. Wu and W. Sun, "High-capacity reversible data hiding in encrypted images by prediction error", *Signal Processing*, pp. 387–400, 2014.
7. Cao, Xiaochun, et al. "High capacity reversible data hiding in encrypted images by patch-level sparse representation." *IEEE Transactions on Cybernetics* 46.5 (2016): 1132-1143
8. Kim, Young-Sik, Kyungjun Kang, and Dae-Woon Lim. "New Reversible Data Hiding Scheme for Encrypted Images using Lattices." *Applied Mathematics & Information Sciences* 9.5 (2015): 2627.
9. Bo Ou et al. "Pairwise prediction-error expansion for efficient reversible data hiding." *IEEE Transactions on image processing* 22.12 (2013): 5010-5021
10. Cai, Siren, et al. "A new reversible data hiding scheme exploiting high-dimensional prediction-error histogram." *IEEE Intl. Conf. on Image Processing (ICIP)*, 2016.
11. X. Wu and N. Memon, Context-based, adaptive, lossless image coding, *IEEE Trans. on Communications*, Vol. 45, No. 4, pp. 437 444, 1997.
12. Xin Li and M. T. Orchard, "Edge-directed prediction for lossless compression of natural images," *IEEE Transactions on Image Processing*, vol. 10, no. 6, pp. 813-817, Jun 2001.
13. B. Ou, X. Li, Y. Zhao and R. Ni, "Efficient color image reversible data hiding based on channel-dependent payload partition and adaptive embedding", *Signal Processing*, vol. 108, pp. 642–657, 2015.
14. H. Yao, C. Quin, Z. Tang and Y. Tian, "Guided filtering based color image reversible data hiding", *Journal of Visual Communication and Image Representation*, vol. 43, pp. 152–163, 2017.