RAPORT

ETAPA 2: Noi metode VRBE de inserție reversibilă de date

În etapa 2 a proiectului, activitatea de cercetare s-a concentrat pe dezvoltarea de noi metode de inserție reversibilă a datelor în imagini criptate care folosesc o etapa de preprocesare pentru a crea spațiu în fișierul gazdă înainte de criptare (VRBE - *Vacating Room Before Encryption*). Mai exact, s-a dezvoltat o nouă metodă de inserție VRBE prin folosirea unor ecuații de expandarea erorii de predicție care permit înlocuirea valorii LSB (*least significant bit,* cel mai puțin semnificativ bit) a fiecărui pixel din imaginea gazdă, indiferent de clasificarea pixelului (în inserabil, shift-abil și pixel problemă). S-a reușit și adaptarea a unei metode existente de VRAE (*Vacating Room After Encryption*) pentru VRBE, precum și îmbunătățirea abordării VRBE discutată în [1].

Algoritmii dezvoltați în această etapă urmează să fie valorificați prin doua articole de revistă și trei articole de conferință. Primul articol de revistă (VRBE cu noile ecuații ce mențin LSB-ul) este în curs de redactare, dar progresează rapid și urmează să fie trimis la *IEEE Transactions on Information, Forensics and Security* (factor de impact: 6.211) în prima jumătate a lunii ianuarie 2022. Al doilea articol de revistă (îmbunătățirea abordării din [1]) țintește accesași revistă și va fi finalizat în februarie 2022. Metodele derivate din VRAE vor fi prezentate la conferințe împreună cu o nouă abordare VRAE.

Activitatea 2.1. Management și diseminare.

Directorul de proiect, după discuții cu mentorul, a stabilit strategia de diseminare a rezultatelor. După cum a fost menționat mai sus, cele două articole de revistă în curs de redactare vor fi trimise spre evaluare și publicare în primele două luni ale anului 2022 la *IEEE Transactions on Information, Forensics and Security*.

Un articol dezvoltat în etapa anterioară (D. Coltuc, I.C. Dragoi, H.G. Coandă „On Preserving Histogram Aspect in Prediction Error Expansion RDH") a fost trimis pentru evaluare la *IEEE Signal processing Letters* (factor de impact: 4.18). Menționăm că aceasta a avut nevoie de mai multe etape neprevăzute de redactare care au întârziat publicarea acestuia. Al doilea articol dezvoltat în etapa precedentă bazat pe inserția PVO (I.C. Dragoi, G.H. Coandă, D. Coltuc „Adaptive Block Selection for High Fidelity Reversible Data Hiding based on Pixel-Value-Ordering") a avut nevoie de schimbări majore pentru a fi

Director: dr.ing. Ioan Cătălin DRĂGOI

competitiv cu noua metoda PVO publicată în [2]. Se urmărește finalizarea articolului până în februarie 2022. Problemele întâmpinate la ambele articole sunt discutate în secțiunea următoare.

Se urmărește si realizarea a trei articole de conferință bazate pe metodele dezvoltate în această etapă.

Activitatea 2.2. Adaptarea metodelor VRAE pentru VRBE

Metodele de inserție în imaginile criptate prin VRAE nu au nevoie de preprocesarea fișierul gazdă înainte de criptare. Acest aspect permite integrarea algoritmilor VRAE într-un număr mai mare de aplicații de tip cloud comparativ cu metodele VRBE. Pe de altă parte, pentru a menține reversibilitatea, VRAE introduce o distorsiune de inserție mult mai mare, iar capacitatea oferită este și ea mai limitată. În ultima perioadă, cercetarea în acest domeniu s-a concentrat pe VRBE datorită gradului mai mare flexibilitatea a metodei de inserție (cele mai relevante articole fiind [3]-[6]). Pentru a menține avantajele ambelor abordări, se urmărește integrarea etapei de preprocesare în algoritmul de inserție și automatizarea acesteia (selecția automată a parametrilor optimi de inserție în funcție de capacitatea dorită). De la VRAE se menține extragerea separată a datelor în funcție de aplicația dorită (fie direct din imaginea criptată sau după decriptare, în ambele cazuri restaurarea fișierului gazdă se face după decriptare). Un alt aspect al VRAE de mare interes este etapa standard de decriptare. Algoritmul de decriptare poate fi analizat, aceasta nu indică în nici un fel prezenta datelor ascunse (un aspect care nu este întotdeauna respectat de VRBE [7]).

În această etapă a lucrării au fost întreprinse cercetări pentru optimizarea etapei de preprocesare pentru VRBE și integrarea acestei etape în algoritmul de criptare. S-a pornit inițial de la algoritmul VRAE introdus în [8]. Acesta poate inserează date ascunse în cel mult 75% din imaginea gazdă. S-a observat că se poate folosi o abordare pe blocuri disjuncte pentru a creste numărul pixelilor gazdă la aproape 100% din imagine. Mai exact, imaginea gazdă este împărțită în blocuri (între 20×20 si 50×50 pixeli). Algoritmul procesează împreună n blocuri, prima grupa de pixeli din [8] se realizează cu pixelii de pe poziția 1 din cele n blocuri. Următoarea grupă este formată din pozițiile 2, iar algoritmul continuă până la ultima poziție ce are o valoare prezisă dată de o serie de predictori anti-cauzali. Detecția se face în ordine inversă față de etapa de inserție (primii pixeli decodați sunt cei de pe ultima poziție inserabilă din fiecare bloc). În prima versiune a metodei propuse se menține structura VRAE. Predicția nu folosește valori din exteriorul blocului curent, astfel blocurile pot fi selectate în orice ordine. Se folosește o cheie secretă de inserție pentru a crea grupele. În fiecare grupă de n blocuri se pot insera m biți, unde m reprezintă numărul de pixeli dintr-un bloc ce pot fi prezișI. Noul algoritm menține avantajele din [8]: selecția aleatoare a grupele

prezise și folosirea a mai mulți predictori (de data aceasta cu context anti-cauzal). Aceste contribuții sunt suficiente pentru prezentarea metodei la o conferință internațională. Metoda a fost apoi adaptată pentru VRBE prin eliminarea grupelor, aceeași abordare este acum aplicată pe blocuri individuale. O etapa de preprocesare (integrată în algoritmul de criptare) asigură detecția prin predicție la nivel de pixel. O etapa de permutarea a blocurilor asigură un grad mai mare de securitate a imaginii criptate. Această idee va fi valorificată printr-un articol de conferință.

Principiul detecției pe bază de predicție propus în [9] (și optimizat în [8]) poate fi adaptat pentru fișiere audio criptate. Numărul mare de eșantioane gazdă într-un fișier audio îngreunează orice abordare bazată pe sortare și grupare. Astfel s-a ales inserția directă la nivel de eșantioane individuale (fără gruparea necesară pentru VRAE), folosindu-se preprocesarea pentru a asigura detecția corectă a datelor prin predicție. La predicție s-au ales abordările non-cauzale existe deja în domeniu ([10] și [11]). Rezultatele inițiale sunt favorabile, domeniul este mult mai restrictiv din punct de vedere al distorsiuni admise, dar predictorii folosiți sunt suficient pe precișsi pentru a permite inserția în straturi LSB. Această nouă abordare va fi valorificată printr-un articol de conferință.

Menținerea după inserție a formei histogramei erorii de predicție (discutată și în raportul anterior) permite un grad mai mare de securitate a datelor ascunse. Un aspect cheie la această metodă este determinarea parametrilor de inserție ce mențin forma histogramei, dar care și limitează distorsiunea de inserție. Histograma de predicție se menține cel mai bine când folosim un prag de inserție cât mai mare împreună cu un prag de uniformitate cât mai mic. Însă pentru a obține o distorsiune de inserție cât mai mică, este nevoie de cel mai mic prag de inserție care oferă capacitatea dorită. Pentru a obține rezultatele optime, se modelează matematic o abordare care oferă aspectul folosirii unui prag de inserție mare prin folosirea unei serii de praguri mici pe un număr de sub-histograme determinate pe baza uniformității locale. Rafinarea modelului optim a fost mai dificilă decât s-a crezut inițial. Menționăm că abordarea inițială, implementată în etapa anterioară, era una mult mai simplistă, folosindu-se un control fin al capacității cu pragul de uniformitate după alegerea unui prag de inserție care asigura forma dorită. Noua abordare permite menținerea formei histogramei la o distorsiune de inserție mult mai mică, deschizând calea pentru o nouă familie de metode de inserție VRBE.

Inserția pe bază de PVO este un subiect intens cercetat în ultimii ani. Astfel au apărut o serie de metode noi cu ecuații adaptive pentru inserția în perechi de pixeli ([2] fiind cel mai performant algoritm nou cu această abordare). Îmbunătățirile prezentate în articolul propus au rămas extrem de relevante (un nou tip de blocuri PVO bazate pe predicție), însă metoda de inserție era una clasică (în perechi cu ecuații fixe). Pentru a pune în evidență avantajele metodei propuse a fost nevoie să implementăm metoda din [2]

și să adaptăm algoritmul propus pentru a folosii noua inserție. Blocurile propuse aduc un câștig în performanțe și pe abordarea din [2].

Activitate 2.3. Dezvoltarea de noi metode VRBE

În această etapă s-a determinat un nou set de ecuații de inserție care permit înlocuirea valorii LSB pentru fiecare pixel selectat pentru inserție (indiferent dacă aceasta era clasificat ca inserabil, shift-abil sau cu risc de depășire). Algoritmul propus împarte imaginea gazdă în două regiuni. Prima regiune are un număr de pixeli egal cu capacitatea dorită în biți. Noile ecuații de inserție sunt folosite pentru această regiune. Se formează datele auxiliare din valorile LSB originale pentru toți pixelii din prima regiune care sunt shift-abili sau cu risc de depășire. Datele auxiliare sunt inserate în a doua regiune folosind ecuațiile clasice de inserție. Noua abordare este una extrem de flexibilă, deschizând calea pentru o serie noua de metode de inserție atât pe domeniul criptat cât și pe cel clasic. Rezultatele vor fi prezentate în articolul de revistă ce va fi finalizat în prima jumătate a lunii ianuarie 2022. Ideea poate fi apoi dezvoltată într-o serie de articole (cu inserția pe perechi de pixeli, pentru capacitate mare de inserție, pe imagini RGB etc.).

Activitate 2.4. Adaptarea metodelor VRBE pentru imagini color și fișiere audio

Inserția VRBE prin substituția de MSB propusă în [7] a dus la o întreagă familie de metode de inserție ([1], [12]-[14]), în ciuda slăbiciunile metodei discutate în [15]. În această etapă s-a implementat o nouă metodă VRBE prin substituție de MSB pentru imaginile RGB care corectează problemele prezentate în [15]. Straturile de culoare R și B sunt inserate pe baza predicției pe straturile derivate $U = R - G$ și $V = B - G$. Predicția pe aceste straturi este mult mai bună decât cea pe straturile lor de bază, astfel dimensiunea datelor auxiliare este neglijabilă (comparativ cu rezultatele pe imaginile cu tonuri de gri). Stratul G este procesat separat folosind doar predicție de pe acest strat (obținându-se rezultate similare cu metodele clasice). Etapa de decodare începe prin restaurarea lui G, apoi valorile din G sunt folosite pentru determinarea straturilor derivate și restaurarea lui R și B. Datele auxiliare sunt inserate în stratul MSB înainte de criptare în etapa de preprocesare, astfel problemele de securitate prezentate în [15] sunt evitate. Noua metodă de inserție va fi valorificată printr-un articol de revistă.

Inserția în eșantioanele unui fișier audio criptat prezentată în secțiunea 2.2 a fost modificată pentru a permite inserția prin substituție de MSB. În prezent se evaluează o serie de predictori anti-cauzali, se urmărește folosirea unui grup de 3-5 predictori pentru a determina valoarea MSB originală pentru un

eșantion folosind 10-20 de eșantioane vecine. Se aleg predictorii care oferă un număr cât mai redus a datelor auxiliare (în care se memorează pozițiile unde predicția a detectat valoarea MSB gresită).

Bibliografie

[1] P. Puteaux, 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.

[2] He, W., & Cai, Z. (2020). An insight into pixel value ordering prediction-based prediction-error expansion. IEEE Transactions on Information Forensics and Security, 15, 3859-3871.

[3] Wang, Yaomin, Zhanchuan Cai, Wenguang He. "High capacity reversible data hiding in encrypted image based on intra-block lossless compression." IEEE Transactions on Multimedia 23 (2020): 1466-1473.

[4] Pun, Chi-Man. "Reversible Data Hiding in Encrypted Images using Chunk Encryption and Redundancy Matrix Representation." IEEE Transactions on Dependable and Secure Computing (2020).

[5] Chen, Bing, et al. "Secret sharing based reversible data hiding in encrypted images with multiple data-hiders." IEEE Transactions on Dependable and Secure Computing (2020).

[6] Wu, Xiaoshuai, et al. "Secure reversible data hiding in encrypted images based on adaptive prediction-error labeling." Signal Processing (2021): 108200.

[7] Puteaux, Pauline, and William Puech. "A recursive reversible data hiding in encrypted images method with a very high payload." IEEE Transactions on Multimedia 23 (2020): 636-650.

[8] Dragoi, I. C., Coltuc, D. (2018, April). Reversible data hiding in encrypted images based on reserving room after encryption and multiple predictors. In 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 2102-2105).

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

[10] Bobeica, A., Dragoi, I. C., Caciula, I., Coltuc, D., Albu, F., & Yang, F. (2018, October). Capacity control for prediction error expansion based audio reversible data hiding. In 2018 22nd International Conference on System Theory, Control and Computing (ICSTCC) (pp. 810-815). IEEE.

[11] S. Xiang, Z. Li. Reversible audio data hiding algorithm using noncausal prediction of alterable orders. EURASIP Journal on Audio, Speech, and Music Processing, 2017.

[12] Chen, F., Yuan, Y., He, H., Tian, M., & Tai, H. M. (2020). Multi-MSB compression based reversible data hiding scheme in encrypted images. IEEE Transactions on Circuits and Systems for Video Technology, 31(3), 905-916.

[13] Yin, Z., She, X., Tang, J., Luo, B. (2021). Reversible data hiding in encrypted images based on pixel prediction and multi-MSB planes rearrangement. Signal Processing, 187, 108146.

[14] Wang, Y., He, W. (2021). High Capacity Reversible Data Hiding in Encrypted Image Based on Adaptive MSB Prediction. IEEE Transactions on Multimedia.

[15] Dragoi, I. C., Coltuc, D. (2020). On the security of reversible data hiding in encrypted images by MSB prediction. IEEE Transactions on Information Forensics and Security, 16, 187-189.