Secure Deep-JSCC Against Multiple Eavesdroppers

Se Seyyle Andriirhossein Andel KKlakhoran † "Mehdi Lettafati" †, Ecenaz Endemir § "Babak Hössein Kkalaj aj †, Hamid Behroozi †, and Deniz Giindiiz §

Electionidal Engineering Department, Sharif University of Technology Telliahrahan Iran

Abstract—In this paper, a generalization of deep learningaidabstigint_mounts chappel soding afficution Sof Cdeap preprinter anded joint rounice tenancial studing! (Deep USCC) approach to secure 2500 manieum dossis studied: hWer propose commend to find (E2E) learning based approach for secure communication against shatiptes elevist represi over combine value on fading i en anver. Both Pseemaries welf edulinating and white containing eavesdroppers aberstudied, Profestive collading tix rategy (ceaves are to peter is have tmend regres republication arithment in a republic for the control of the control ensumble learning met hod, while for the uni-colluding setup they he furtione. PThe goal its to prevent reaves droppers from inferring private, (schistrive) i information manout the a transformated innaiges; while delivering the intages for regittimate we delver with thin intern distortion. By generalizing the addissor proving finally had wretho emanner coding; the tradelarit between the analyst recovery at the legithmate node and the information balkage to the dayesdroppers is cenaracterized: a To vsotke whis melowego faloret of ramework, owe implement deep near at networks (DNNs) to realize at data driven seithrent combination on sensifie, datenolist richytige on Signal phicans tiata distribution. Simurations over CIFAR 100 dataset verifies the SedveevoninhtyogranicompfAntversdraapaeenraevolop eavesdrappers Brevatsolstindicarover Rayleight fading, Wakagaminn, cand AWGN thangues to verify the febrerateurion of the proposed scheme Our experiments is a conditional transfer of the complete and the condition of encouring tan decrease the adversarial accuracy by 28%.

Index Terms—Secure Deep-JSCC, data-driven security, secrecy-utility trade-off, secure-image-transmission.

I.I.INTRODUCTION

Driven by the growing interest in semantic communication priven by the growing interest in semantic communication because of its various applications in augmented virtual reality after the properties of the delivered contents of the growing in a security of the delivered contents to an and success of such services rely highly on the security communication systems should understand the desired contents of the delivered contents should understand the desired fixed of security and intelligently adapt the transmission scheme accordingly the desired "level of security" and intelligently according to the desired "level of security" and intelligently according to the desired "level of security" and intelligently according to the desired "level of security" and intelligently according to the desired "level of security" and intelligently according to the desired "level of security" and intelligently according to the desired "level of security" and intelligently according to the desired "level of security" and intelligently according to the desired "level of security" and intelligently according to the desired "level of security" and intelligently according to the desired "level of security" and intelligently according to the desired "level of security" and intelligently according to the desired "level of security" and intelligently according to the desired "level of security" and intelligently according to the desired "level of security" and intelligently according to the desired "level of security" and the desired "level of security" and intelligently according to the desired "level of security" and the desired "level of securit

adapt the transmission scheme accordingly of the most significant driving force in telligence is foreseen as the most significant driving force in telligence is foreseen as the most significant driving force in telligence is foreseen as the most significant driving force in the sense of the

ever-rising attacks, such as eavesdropping, spoofing [?], anRegentlyn-theonsiderable number of research has been dedleated by the outilization left deep dearnings (Dich the briggers the diptimize the hoerfolization off where less essentions. Dhanks cho their outstanding performance and generalizations capabilities { Plan [R], t[d] | Heirthendottexting wireless security, dagto encoders técomposedbioftifinear, layers[?] ar en exploite ditinxt[?] f ovéreltse additive, white Gaussian noise (AWGN) winetap channel. aTe tackleitthe itrade-offebetweendtheiwlatwhiate Gadssecurity is a (welly lifed) sume of a block perior Trates and information fleakage eis tised last the aloss function (LyF) of ore ignited wire tapf colde idesign: Take datal fedfonto also autoekegdeis is combined exliths additional (ibfr-) informative wandom thitse the significant that and window thitse the significant in the significant was a significant to the significant was a significant with the significant with the significant was a si swhite; (this labs) is reduced the continual idation between Notably, aniost of the oprovious works eithe [24v43 dr 45 before hibn teasing) aided-sectire channel-goditign rather, than taking rintet account the endstovenck (E2E), performance, of osecure redemminigations. Telegroon tentroff the draps mithed that a is a kongail dressed oing the se worktspandch(E2lift)rebif-streamois equality treated as the secret information toobet protesteshagainst dart eaves dropped ressed in th@hevE2Excommuthicationroflittagesafrons accourbe node ad as legitimater destinations tiam beocons identified a joint isource ehwendt opderg (JSCC) problem. DL-aided JSCC design, a.k.a Delib dS EQE has meocived trignificant nattention thanks storits superion pelformance: charticularly des lackconsirbiance son acientrase uchannela istate cinflorga (ith/C[2], pHowlever, InL-ISC(cl. dBfccentesign, separateDoupedS60Cchannel coding, thig affannel andeword is corkelated with the underlying source signal. This itan lerdatefyndherabilitie súrcteratis of de akalgettote avelalroppiers, despito vproviding J&Bustnisse against achannel atoise uluspined blys(nh) eindo(dh) gyet providen a glenoridization sof the eDeepl-J&CC approachetly seguroucom signication i problems against multiplie eaveadroppersofte this gegarda (2) proposes, algeberative withing satialstnetworkg (GAN) linspired securd mentral leheoffer dedoffer pair joveri die AVgGiN swiretajoch aufneh aglitenspolfe@avesdroppeh The eauthors imply hipropose parobriation ghiautoemyltdele (VAE)based approacht for Deep-dSSC designoswerabigany sytinmetrile channels, againochnsiderhig jassingle cavesdropperal encoderdelin dhis paipenywe consider N2Eitetanjingsbasell againstcome enweightigg og affisternultiple save silfoppers der bothscolluding ando nonocleti(di/dgE) edwesetroppors,a dwebr AWGNJSiSCwlettigas fadin bichannelsu Fort the cleenarile, of good luding chaves dropperly; the adversaries share their logits to collaboratively infer private attFibutes based on the on side of the leadering of the leader of the le

[†] Concomposition to the Engineering Department, Sharif University of Technology Stellicht ann Iran Department of Beteine and Bestronic Engineering Imperial Collegie solden OK UK

Emzilia ilk mitmeatifine eco benozi 2 ek kalai (19 sharif edu); jameli @ee sharif edu); s{ e-entelmei 7, 7. gunuuz w hijienari ieluc uk

^{*}Equal contribution

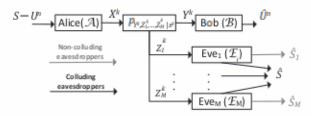


Fig. 11: Přoposededystentemodelo ful sécure-etransmissionnigainst ngalúple cawbihlopperses droppers.

formthennon-colluding netuputhey lacta alone of Please (see) Fig. 23] for an illustration of the communication scenario Audied in this papead Application's of outhproposed frameworkling elude (fbut pares, note limited sto) edigitale health carets cryice Natio which the digal imagese are taknitho basterelyed bfroms access points newhile resorbe vehillate or attributes, collecting identity hof patients_should_be_kepti_secret_from_potential_eavesdreppers. Notably, previous, works, [R] and [R] sonly considered, a single eavesdropperd with newingle autenna (transmitter (and multiple pagallel schannelsrerespectively:nInvadditionschoth fillhand 424 are thin ited reseated channelses Moreover, whife rent from vh2 le not additional, gedundant bits tore required to sho addedeto; the source image. Jordhis paper, Rayleigh fading channel model isouted [to representatione-warying rehannel realizations during training, swhile-inference is spenformed soutra Nakagamis maand AWGN|shannelscrip/edditionaddRayleighdading| Note that the imaged and the decoder do not require any knowledge of the instantaneous, cheenel gains linethe proposed eschembe added to the source image In this paper Rayleigh fading thannel model is used to represent time-varying channel model is used to represent time-varying channel Consider the communication scenario depicted in Fig. ?? realizations during training, while inference is performed where a multi-antenna source node, Alice (A) with n a antenna source node, Alice (A) with n a antenna wer Nakagami-m and AWCO channels, in addition to nas, aims to deliver an image U EU to a desination node, Bayleigh fading Note that the encoder and the decoder Bob (B), over k uses of the communication channel, where U do not require any knowledge of the instantaneous channel denotes the alphabet of source images. According to the JSCC gains in the proposed scheme. gains in the proposed scheme interature [7], we refer to the image dimension, n, as the source bandwidth. The champel dimension is plaracterizes, the channel bandwidth, where we usually have keen neto reflect the concept of bandwidth compression (2) Image delivery should be kept $segret_n$ from i multiple erayes droppers e denoted by Exed(\mathcal{E}_{t}), maticEvenu(Embowhish, overhearuthes communication intrough their rown what nels denote wante to hinter en private c (sensitive) attributenge.go diagnostic information regarding of the tsource image, denoted by Sactisc with a discrete alphabet San The gayesdroppers in the non-colluding setup actual one to infer the secret, S. p. hile, for the colluding setup, "knowledge sharing it is also performed they share their logits based on the concept Ω on semble pleating depends denoted by $\mathrm{Eve}_1(\mathcal{E}_1), \cdots$ EvAlige maps the source information $d_{inicintora}$ tohannel input concernations, and want to viscera presidence function $f_{\mathcal{A}}: \mathcal{U}^n \to \mathcal{X}^k$, where $X^k = f_{\mathcal{A}}(U^n)$. Transmitted codeword ¹Notations: We denote the transpose, the conjugate transpose, and No fations in Wed denote the transpose, (the conjugate transpose, and by night of pevdetdr/bylu(e)dn(-) he and () a bill itesphenisitly. (The texpected yable and the probability (#8/isityXfunctionl (pdf)edf rland@inXfariable (RXV)xX, are spentited by Ricklizatdon wischorespectivelyur Realization togetors but of RVs were applied total By bolds towerbaser letters in The Bristual and driffationd offi RVs of sentiropyand the criss-ehubjynofytwo digtributions/ynand-sparei/shlywhyre&feCtiVelya.bd

 $H(\mathcal{Y}_{p}; \mathcal{Y})$ and H(p, q).

ist stibject, to .gn, alveragespiowerf.constraint regEr(dXfg) $t Ne^k s$ our Dewhich, with the delatis field. So with a realistational of ather chaffiles eadewbrobjier our tdata-drivenlladjirgasht uChannelbioutputs for Branchofet are denotethered special blyling setuand "Zfovdeoffe whithing" is also perform Edanshiss idm of thata-strains over the the experiences independent realizations of the conditional channel distribution $p_{Y,Z_1,...,Z_M}|_{X}$. We consider both the AWdise and is other parties of the standard of the standard working the standard of the standa Nakagami-m-channels, hard assume the channel realization to Fernameronsian rebittie direction of the transmission of a stringte intage, i.e., You for for channel insesy Bob thent appries are decoding plization groto the tail a time code word Meanwhile teach i Eve approachtract the sensitive attribut Santon her observations Z*Peofi bel veoliaborating with other Evel, Te. sharing their logits. We consider the trade-off between delivering infrages to inderwand the mightest invening after connectining a his hard market in the connectining a his highest in the connectining a his highest in the connectining a high particular market market in the connectining a high particular market teakutiono neago advertary. Wonsen sidore brette afte Awasurea by aley, fading obannels, where farshersly usading by quelept taga widehvasechmeelete p. Wearleigte Fading and Sukugaroh rrachework to endrasserize this chargost, realization for an service *consta*nt high rithmed was in most work transmission of masing le itriven, mander by hannelnesen Bobbben wardenatieany liwe famctioshm*la*taheoustvillinimize bela (the distortion dilen gach Evideriand onextraormation quaktive, at (5:15249), Single of materials adversations This corresponds to the region with other problems, i.e., sharing their logits. We consider the trade-off between delignting cim geo (UV BOb) with the highest (SdZhty and controlling the information leakage to each adversary, which is theoretically measured by the mutual information where $w_{\rm pv}$ shapes our secrecy funnel and adjusts the trade-off metric T(S, Z). Inspired by the key idea of privacy between the information leakage and the distortion. Numerical runnel [1] we first formulate an optimization framework solution of optimization (??) is intractable due to the mutual to characterize this trade-off, which we call secrecy funnel information term. Hence, we apply a variational approximation This funnel-like framework is then solved in a data-driven of mutual information, which was proposed in [?]. Then, our manner by implementing DNNs. Mathematically, we aim optimization can be rewritten as: at Bob, and the information teakage $J(S, Z_{pm}^k), m \in [M]$ thadwersaries. This corresponds to the following problem

minimize $\mathbb{E}\left[d(U^n,\hat{U}^n)\right] + \frac{1}{M}\sum_{w_m} w_m I(S;Z_m^k)$, (1) where $d_{S|Z_m^k}(s|z_m)$ characterizes the e layer, is posterior estimation corresponding to the correct distribution of B training the observation Z_m^k and the factorized by DNNs with parameters Ω_m and Ω_m are parameterized by DNNs with parameters Ω_m and Ω_m are parameterized by DNNs with parameters Ω_m and Ω_m are parameterized by DNNs with parameters Ω_m and Ω_m are parameterized by DNNs with parameters Ω_m and Ω_m are parameterized by DNNs with parameters Ω_m and Ω_m are parameterized by DNNs with parameters Ω_m and Ω_m are parameterized by DNNs with parameters Ω_m and Ω_m are parameterized by DNNs architectures and the training strategies are given in the next section. The variational approximation of mutual information, which approximation in Ω_m can be interpreted as the sample-wise negative cross-entropy (CE) between the distribution over rewritten as: adversaries predictions and the true distribution of sensitive attributes: Edstolve Ω_m in a parameterized by Ω_m and try to infer the sensitive attributes of the transmitted images where Ω_m parameterizes the adversarial network of Evenwhere Ω_m parameterizes the adversarial network of Evenwhere Ω_m parameterizes the adversarial network of Evenwhere Ω_m parameterizes the distribution of Ω_m given the observation $\Omega_m^k = z_m$. To realize a data-driven approach, Ω_m and Ω_m are parameterized by DNNs with

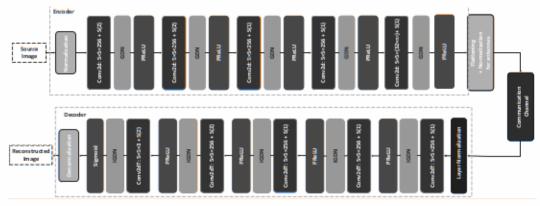


Fig. 2: Proposed NNN is AticA (encoder) and Bohd devide(decided entropy at the encoder) at the encoder of potential and the encoder of t

parameters Ω_A and Ω_B , respectively. Details of the DNN architectures and the training strategies are given in the next section. The approximation $q_{\rm ing}(??)$ can be interpreted as the sample-wise negative cross-entropy (CE) between the distribution over adversaries' predictions and the true distribution of sensitive attributes. To solve (??) in a data-driven manner, we assume that the Eves also employ adversarially-trained DNNs and try to infer the sensitive attributes are also employ adversarially-trained DNNs and try to infer the sensitive attributes the adversarial network of Eve_m. Accordingly, we Accordingly two local formulated. The following LF.

$$\begin{split} \mathcal{L}(\Omega_{A}, \Omega_{B}, & \Theta_{E}) = \mathbb{E}\left[d(U^{n}, f_{\Omega_{B}}(Y^{k}))\right] \\ &+ \frac{1}{M} \sum_{i \in [M]} w_{m} \max_{\Theta_{E,m}} \mathbb{E}\left[\log q_{\Theta_{E,m}}(s|\mathbf{z}_{m})\right], \quad (3) \end{split}$$

where $\Theta_E \stackrel{\Delta}{=} ((\Theta_{E,1b}, \cdots, (\Theta_{E,Nd}))$, and $q_{\Theta_{E,m}}(s|z_m)$ formulates the approximated deversarial iddelibelide organization of the mathematy. Details so fifth proposed DNN architectures and the training strategies argies were given following leaving. section.

IIIII DNNNA Aceintectrures

According to the Deep ISASC Concept [2], [We umplay law toetreoderdDNDs\tisdirectly ently theaimage pixelsetoichdantel input symbols. Us this regards. Almapsegach, realizations of able soulizatdata δf^n thde notedobylati $\in \mathbb{R}^n$, the noted by $\delta \iota$ charitrel input/xecfoE of which real i bowiewell as a realization of eX/fe/Feb block reliably attion of the XDNN shemble yeed for the negutile encodes and decode components of deglt imatel parties is illustrated in Figle@2.inImadditiotieshis DNN:structure FigpR@ednbwdzhichoof the adversaries is the adversaries is deAccordingeto the proposed system model, adversaries utilize DNNs otol if agilitatel the ninderences of togen situade in formation in & frtifizethEINNescivefacilistrate, tSecanfebenthe of associables of fthe images [3],fr[3]). For example of height stiff of apalients within Inedisablirtiaging sinese-fiealth, applications of the federentiative attributes within images aleach gady erasylventhlogs of the aDNN architectusenilltistratedrilnuFig.fr23n wherestheadimensionapf

the output neurons, L, equals the cardinality of the secrets |S|.2 The output of the softmax layer produces an adversarial likelihood estimation regarding the posterior distribution $q_{\Theta_{E,m}}(s_m|z_m)$. Invoking (??), one can say that each Eve tries to minimize its CE between the adversarially estimated posterior distribution $q_{\Theta_{E,m}}(s_m|z_m)$ and the ground-truth, which is represented by the one-hot encoded vector of S, denoted by $\varepsilon_s \in \{0,1\}^{L_0}$ Notably, having lower CE values results in higher similarity between the adversarial posterior distribution and the ground-truth, which increases the informa-Fign feakage meterns of CE. Meanwhite, 121 and 18 tily to juility minimize the reconstruction distortion and the information leakage, measured by the negative CE metric. Hence the sample-wise communication framework can be reformulated the dimension of the output neurons, E, equals the cardifality of the secrets $|S|^2$. The output of the softmax layer provinces $\mathbf{z}_{\mathbf{u}}$ (algebra $\mathbf{z}_{\mathbf{u}}$) is blood at \mathbf{u} at \mathbf{u} at \mathbf{u} at \mathbf{u} the posterior distribution $q_{\Theta_{F,m}}(s_m|\mathbf{z}_m)$. Invoking (??), one can say that each make the qop instrinize its, (4) between the adversarially estimated posterior distribution between the adversarially-estimated posterior distribution where $u = \int_{\Omega_c} u dt$ and the ground-truth, which is represented where $u = \int_{\Omega_c} u dt$, and p(u,u) stands for the joint problem, the one-hot encoded vector of S denoted by $\varepsilon \le \varepsilon$ ability distribution of the original and the reconstructed in- $\{0,1\}$. Notably, having lower CE values results in higher age, taking into account the randomness in the input image shullarity between the adversarial posterior distribution and the channel. Since the true distribution p(u) is often and the ground-truth, which increases the information inknown, we estimate the expected distortion measure using leakage in terms of CE. Meanwhile, λ and λ try, to samples u_1 from an available dataset λ by computing jointly minimize the reconstruction distortion and the Equation λ and λ try, to samples λ and λ try, to sample λ and λ try, to sample λ and λ try, to sample λ and λ try, the reconstruction distortion and the Equation λ and λ try, the sample λ try and λ try ngormacion leakage measured by the negative CE metric. Hence, the sample-wise communication framework can be which the cavesdroppers are interested, as well as their channel models. Both of these assumptions are common in the privacy [?][P[P] and whetap chantel[?]; [P](.[2]) [deraude] We do not need to know the instantaneous channel gains, but use their distributions to sample channel realizations during training.

Training Proceditie. In order to train our system based on (??), we follow an iterative procedure. Intuitively, the network nodese are faced (y)thadminimal samels for the competition between legitimate autoencoder and the adversarial DNNs.

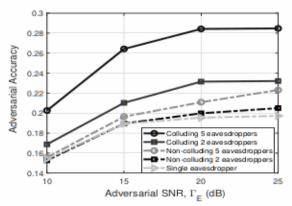
²It would be interesting to study the performance when the earlistically bis interesting interesting, this performance which tithet caves droppers dropped and order interesting the interesting of the second order. Heilite; this following strategy is gunathrough lour proposed dE2H system: (Ehérenénder and) dec oder function nefsAfrice landnBob should sould sould the initial theoretical by the stribution p(u)is often unknown, we estimate the expected distortion measure using samples u_i from an available dataset D_u by computing $\mathbb{E}_{p(\boldsymbol{u}, \hat{\boldsymbol{u}})}[d(\boldsymbol{u}, f_{\Omega_{\mathcal{B}}}(\boldsymbol{y}))] \approx \frac{1}{N_{u}} \sum_{\boldsymbol{u} \in \mathcal{D}_{u}} d(\boldsymbol{u}, \hat{\boldsymbol{u}})$ where $N = D_u | D_u | D_u | D_u |$ where $N = D_u | D_u | D_u |$ where $N = D_u | D_u | D_u |$ where $N = D_u | D_u |$ where $N = D_u | D_u |$ attribute in which the eavesdroppers are interested, as well as their channel models. Both of these assumptions The draining process of legitimate modes can be afurther and Râncéd via employinge.adwersakialn likelihodd toorkpensatibn (ALC) tambiols has about shown in [?] use be enord of febrive in confusing an adversary than the one-hotten coding approach. The main idea is to make the posterior distribution of adversaries imitate a uniform distribution $\bar{p}_L = [\frac{1}{L}, \dots, \frac{1}{L}]^T$. Heffcein Alic Prand dBob. Jointlylemanitrizer the unsertaintys of adversarial predictions, an sulting tinethe following loss distinction the network nodes are faced with a minimax game, i.e., the competition between legitimate autoencoder and the adversarial DNNs. Hence, the following strategy is run through du hopsed E2E Hygueni (Stud Zonduder had decode Pfunction of Arice and Bob should jointly minimize their LF, denoted by \mathcal{L}_{AB} :

The distortion measure we consider for our legitimate loss function \mathcal{L}_{AB} is a mixture of the average mean squared error (MISE), denoted by Δ_{AB}^{MSE} , and the structural similarity index (SSIM), between the input image u and the recovered version u at the output of Bob's DNN. Therefore, we assume $d(\cdot, \cdot)$ to be measured as follows

The training process of legitimate necks can be further enhanced via employing adversarial likelihood compensation (MsC) \dot{u} , which has been shown sign [2], \dot{u} be more effective in confusing a uning parameter representing the encountry approach of the SSIM metric. The SSIM measure between distribution of adversaries imitate a uniform distribution two images $\dot{p}_L = [\dot{t}, \cdots, \dot{t}]$. Hence, Alice and Bob jointly maximize the uncertainty of adversaries initiate a uniform distribution $\dot{p}_L = [\dot{t}, \cdots, \dot{t}]$. Hence, Alice and Bob jointly maximize the uncertainty of adversaries in the process of the proce

where μ_I , μ_K , σ_I , σ_K , and σ_{IK} are the local means, standard deviations, and cross-covariance for images I and K, while c_1 and c_2 are two adjustable-constants [?]. The rationale behind the proposed distortion metric is flat we not only aim to recover every pixel of images with minimum error (captured via the MSE measure), but also want to obtain a good-quality reconstitution from the human perception points of victimate lose a finite professional transfer of the Branch professional transfer of the Branch professional transfer of the professional transfer of the professional transfer of the Branch professional transfer of the Branch professional transfer of the professional tra

where $\mathcal{L}_{E\Delta}$ MSE $\underbrace{\frac{1}{|W_u|}}_{i}$ $\underbrace{\mathcal{L}_{i}}_{n}$ $\underbrace{\mathcal$



FigFig. ToTotal didversarial accuracy/over Rhylgighghalmelsiels.

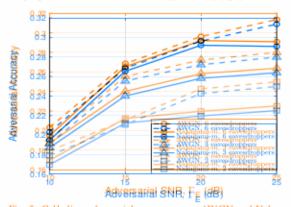
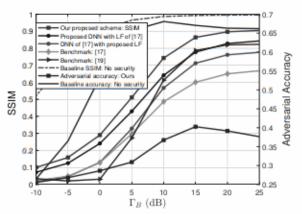


Fig. Fig. 5: Colluding adversarial accuracy over AWGN and Nakagami.

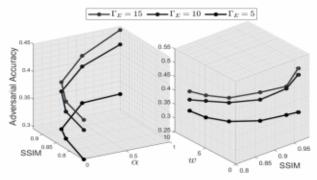
for the case of colluding eavesdroppers, an additional step of knowledge sharing is performed. In this case, the adversaries share their individually-extracted logits) (and a weighted sum of these logits is exploited for the inference of private attributes. where the logit weights are trained in the colluding framework where μ_I , μ_K , σ_I , σ_K , and σ_{IK} are the local means, K In this section, we evaluate the performance of the proposed rationale behind the Desposed distortion metric his that scheme over both AWGN and complex lading (Rayleigh and Nakagami-m) communication channels. We address the generalization capability of via proposed scheme for different want to obtain a good-quality reconstruction from the communication scenarios and over a wide range of signalto-noise Patro (SNR) Values, to highlight the data efficiency of Each pitchosed thearining-basening-culing-toolsum tower also audrels vind sex recytaintive ration of rothine proposeinteaning-based approach, we evaluate the propose a Secure transtwork estimated likelihoodingension \$ 321 \times 320 \times the (ground width ensimers) from curaring dataset Prome datasel evisis is of 60000 corose d Integrishing size 32 × 32 fixers. The training and evaluation sets are two completely separated sets of images, containing 50000 and 10000 images, respectively, associated with 10 classes. Adversaries wish to infer a common secret Specificant individualitys actional and a contracting eclassion of by pearling Arberther temperation of when access are notices, one editional stermon The colonians beciens 3 in over forward detecth is one or take od CIFARe40 hmagde with distidually-extra Fordsingific involve woistekedassing of wheren locitic is explaited for the informac Wepalsotsetabtributesand her eit bealuginaseiThoseaparameters inether after bendueting extensive experiments and training the DNNs with a wide Fangler and for alues for w_m and α , where we have omitted the results of fine-tuning step due to space-limitations, Transmit SNR wef communication links are defined as Ind Nakalesmi + OBunnel Figation Olyson of the representing the ratio of the average power of the channel input tehtheraveragerneiserpowerrofriegitimate, $\sigma_{\rm paands}^2$ adversarial $nodes_{\parallel}\sigma_{Ra}^{2}$ respectively, During training we set $\Gamma_{Raltie}20dB$ and light thid Blarespentively, while we test the performance nyer different values of channel SNRs during the inference; In additions the bandwidth compression ratio is act to Force! For the training two sample channel realizations from the general case of complex, Rayleigh fading model (with average, Limand Frony dury stated datase. Nevertheless, during sites informed phase-wenstudy the iperformance pine different tescenarios and AWGN; and Nakagami-tw-shannels (for msep 3) aWhile we do assume, knownichannelomodelsi inoomosimulations.stychich-eye use to generate samples from conditional channel distribution. we could easily drop this as sumption if we had data collected from a particular channel with unknown statistics. DNN architectures are implemented using Python3 with Tensorflows The sodes were run an Intel(R) Xron(R) Silver AHA (CPb) running ati 2,20sGHz with GeFpree RTX1;2080 Tie GPUs To minimize the JLFs in the widely adopted Adam poptimizer, is suchosen [2] with a learning rate of about 10 fixethe number of training spisodes.nouNeimodext 200 vandsthe ibatchesize dotra imid28 he Divigs. with and will show the adversarial acquirect, of the proposed schemed validhees NR of radversarial links (Fig. to Frace 5 idB) after both seenances SN Rolleding and non-colluding gavesdroppers. For the colluding segun, the total andversarial agguracy, refers to the overall accuracy, of adversaries in correctly finding the ground-truth and from their aggregated logits while for the non-colluding benchmarks, the mean accuracy across, envesdroppers is plotted for the sake of comparison. One can observe that increasing the number of caves droppers leads to higher accuracy for the adversaries, which is aligned with one's intuition. The increase in adversarial accuracy is more significant in the colluding case due to the collaboration and, "knowledge, sharing" among cayes dropners through the ensemble learning process [2]. This actually helps them learn the secret more accurately. The figure states indicate that by inoreasing the quality of adversarial links of emincreasing his the accuracynef kadversaries ingreases by at one stirle Wati This istherause bigher SNR avalues result in baying less distorted (less-inoisy), observations at the envesdroppers resulting in more accurate estimations about the iposterior adversarial distribution tagestics DNN The hamounter of ringressen in the adversprial accuracy reduces with the increase in Fe which highlightsxthendignitation of regression ppersion the appropered secureCacheme. Rfig. 2020also chighlights ather generalization capability of our tearning based framework extended to the AWGN and Nakagami-m (for $m_x = h3$) channel scenario ut shows that we can achieve almost similar trends in change scenarios other than Rayleigh fading despite atraining, the networks with a Rayleigh schannels model of adversarial links



FigFig. AbAblation study for $M=3\,$ non-collading gaves dsdpp: p.ers.

(FFig= ?f rillustrates) the data bresonstruction performance rat Bob-anduther total addressmials accurate when they ingtell, #h3 non-boldbeing reaves droppers r Ones can tinfer from the digure that our proposed system outperforms the benchmarks in terms of the reconstruction performance: Accordingly, 20% and 40% berfohmands, gaine is a sahieyed abye our oproposades chempeeoms paredewith [2] and [2] of spectively. The ablation examinations conducted in this figure show that both the implemented IDNNs and the proposed LEs for optimizing the framework contribute to the system seed on an engage and the three seed on the system of the seed of the system of the sy The ifigure also limplify that increasing for tresults inchaving higher SSIMe values h. This ets begause ingreasing Tens can result imeless sdiatottede abservations eas Bob. Which decilitates ethe image reconstruction performance. Data efficiently and sino endlizabilitya of our proposed escheme lare also (validated,) since we have trained four DNNs withou fixed SNRaFigs inc20adBs while the performance gain; of low, approach, during Enference heldst for varioug SNRsLiFuntbedmores Figis?? bigblightschataf we ignore the payer droppers during the atraining of tAnAtpairs and set the posterior & Mesouraproposed scheme can achieve almost-perfects(SSIMase it) (data/recoveryalTiberimpsyctedfithe eaves dropperseone Bob's, performance jean, beastudied, in this figure das well-swheth having 3ecase edroppers can impose 10% decidashtinthe reconstruction performance of oBoble Finally. torsindicate the oith portange of country proposed adversary aware schefne in terms) of preventing leakaget, we can observe from the figure that if swelde not employ becaut neural jeacoding than ignoring the diages dropperst during the training lof vAtB pair), the adversarial accuracy is increased by about 28%. This clearly highlightsathe importance of compleying our proposed learBirlg-based lsective acreeding as chemecuracy, when having MFig.3 ??ostudiesdthg impactropptensin@parameterserxfrand theorfighteadversarial performances of tour proposed is within Thosh rhypes-parametersoarch the ecoefficients rassociated a with utility dind [sec2009] adjustment ptermen within goin training election by (?d)randr(38), ere spectively. Contained xperiment, the idd/etsocial operformance also attoured aby ninvestigating (the decouracy figuadversariestlia teorrebityhfinidinglethenground-NNth dabett be (nepresenting Pthe sensitive information (S) namons: the labels to 6 CJFAR-sl@tdatasetieThe_figure_indicatesethat jby_inbreasingchhighes.valluesfofuSSBMscain/bejacttlexed.nsingesimorE emphasis

³https://www.tentorflow/bag/.org/



F Eig.77:Secreey-atility tradesoffiff

in having higher SSIM values. This is because increasing the SSIM error SSIM is but based on 1999. However, if aceuracy of adversaries in extracting the sensitive information facilitates the image reconstruction performance Data officiency band generalizability of our proposed or heme are also validated a ince we have trained our DNNs with a fixed $SNR = B_0 = 20$ dB, while the inerformance gain of choosing '\(\alpha\) =0.1 for our network. Similarly, by increasing on, the emphasis goes toward the secrety cherry involuced in First harmore (Fig. 22), which leads to the reduction in adversarial accorded as well from the adversarial accorded in the accorded in the adversarial acco in this figure as well where having 3 gaves troppers can in payer and figures based for econstruction sperformance, of Bob. Finally, to indicate the importance of our proposed adversary-aware scheme in terms of preventing leakage, we can Vol GONC flus MONSE AND THE UTHER ESTIMAN SEMPLOY secure neural encoding (i.e., ignoring the eavesdroppers during the training of A-5 pand, the adversarial accuracy image_delivery_against_multiple_cavesdroppers;over_lAWGN and complex-yalued fading channels by ded considered both scenanos of colluding and non-colluding eavesdroppers over CIFAR-10 dataset. For the colluding strategy, eavesdroppers collaborate to infer private data from their observations (channelecutputs), using netsemble learning entitle to a special out colluding setup, they act alone, Meanwhile, the legitimate parties aim (to) have a secure communication with minimum average distortion Employing autoencoders we proposed a secrecy funnel framework to achieve both secrecy and utility where two also take into account the percentual quality of image, transmission within April J.F. Eyaluations validate the performance of our proposed scheme compared with existing benchmarks, while addressing the secrecy suitity trade of hour proposed system; is also shown to be generalizable to a wide range of SNRs and different communication scenarios, which ve Fature Directions in Air problemoto Nect studied in ctraining the systems over real time wireless channels. The challenge herenis, the relatively long coherence time compared to the rate out. Which relats is samples Is an abee punces seed of fore trainings Accordingly; only a few channel realizations are observed over eyery (minibatche)which will be an important is sue for training communication systems that are supposed to generalize well to all wide range to be channel it is aligned in the same Γ_E can improve the adversaria errences finding the sensitive data of grid and sensitive data of grid and sensitive that accurage. For the sensitive that the communications of accurage the sensitive and task-priented communications." arXiv:2207.09353, 2022 the lamitation of adversarial nucles has end of communications accurage proposal secure receives the metaverse: An overview." Ad Hoc Networks, Aug. 2023, https://doi.org/10.1016/j.adhoc.2023.103262.

[3] Q. Yang and D. Gijndiz, "Coded caching and content delivery with heterogeneous distortion requirements," *IEEE Trans. Inf. Theory*, vol. W64, propaged 347-1866 m. ing-2018 ed approach for E2E sectiffeMndagkewikeli PerGündüzinad Kraftikolaiczykyé3Mirelesseinagever AW (10) Jan 2020 in plex-valued fading channels. We consiflerMdLebotth HsBehaviosBoff, Khalaiding E.aa.doweisek.ol@oding eavebased poedical image (transprission) against sandordy-distributed passive eavesdroppers," IEEE Int. Conf. Comm. Workshop (ICCW), Montreal, strategy, acquest poppers collaborate to infer private data from their pole annual is used (chan unker usunt m) agus insus usus user for ble delayaware systems froith trandomly-distributed ceases dropners of IEEE Trans. Comm., vol. 70, no. 2, pp. 1125-1139, Feb. 2022. secuFenweis; undiHcWtiPoor, wt/dmextin/imeisecutive forg6Gdis/telest/iThe Emphly if ghysical large gravity w202 brog 8652401a01556 ecv. funnel [8] M. Letifati, H. Bebroozi, B. H. Khafaj, and E. A. Jorswieck, "Hardware-framework PHY secret key generation with man-in-the-middle adveralso strike" IEEE Wirdenntonine Liner veh tuahoq4 alipty856f860n Age trans²⁰²²ssion within our LF. Evaluations validate the per-19 M. Letafan, H. Behroozi, B. H. Khalai, and E. A. Jorswick, "Deep formance of narroward more and compared compared compared by the compared of bench-mankishwhileta,"dd@ssinge thebsecommunitalitys:tCaderoffe Our GAOBESOM's Madrid. Spaints Decs 12024 nprol to generalizable [10] E. Bourtsoulatze, D. Burth Kurka, and D. Gündüz, "Deep joint source-to achange country wireless in age transfersion," (PEEP Trans. Cogn. scenazios. Netw., vol. 5, no. 3, pp. 567-579, Sep. 2019.

[11] D. B. Kpke and D. Gündüz, "Bandwidth as ile image transmission with deep joint source-channel coding," IEEE Trans. Wireless Comm., vol. the systems of the systems of the challenge highers that are left Barbyodoria, Hokkerbiggood line, doministed Wireless rate powered cooperative key greeration for chealth: A reservir learning approach," 2022 IEEE 95th, Vehicular Technology Conference (VTC-Accopying) Helsnity, Pintania, 9th 1902, pp. 12-p. tions are observed two Keyler Bessen Boalich, with high and had and large transitions are observed to the conference by neural network subsequences the Earl interpretation for transitions of the conference of the

- Secur., vol. 15, pp. 3374–3386, Oct. 2019.
 [C1] CRAPTISCHER, R. P. Schaefer, and G. Winder, appeal realizations and coding via neural mutual information estimation," in *Proc. 20th Int. Workshop Sig. Proc. Adv. Managem Comm.*, pp. 1–5, July 2019.
- [15] R. Fritschek, R. F. Schaefer, and G. Wunder, "Deep learning based [1] Wirefulpudding visiting and Establish distribution on the Visit Annual Company of the Visit
- [16] F. Main 280 76 (1985 East 2024), and D. Gündüz, "Adversarial networks for
 [2] Meure Wirefels communication 2 "PROPE Int." (Vonf. theoret proven Signal Provents (ICASISP), Barceloha, Spain, 2020, pp. 8748-875 2 net averse:
- [17] AnErdemics Ridw Dragodicland DloGündiDiet Privlisty-awalengomm26123http://doi.org/10.1006/j.withbeen261614-18663-ks." IEEE Int. Conf.
- Quality Spend Storadia discuss Ocass Problem and Sunday Singlipers;
 Mish 2022 pgc 2080 s 2004 ortion requirements," IEEE Trans. Inf.
- [18] BhBorKurkal afid, DroGfindija, "BéöpJSEC-f-J Deep2ftößt source-channel
 [4] McGilgrostrimkije Dwiffi ifelößbacket WEEB ikolojiatyda, "Wiendest innage.
- testimenton Theoryckyel." IEEE IJphel78-499; May 2020vol. 39, no.

 19] R. pelikkir, 10Bodstrap Wipired techniques in computational intelli-
- [5] Mindelt Milli, SkyrMeProcesis, Magl. vish24a jnornal pp. 59-72;r2007ck.
- [20] AC Middiddumid SneShlanhattang Ntr Fawmissiand Mai Médand de Folym distributmations souteneckes de dep privacy liftiniel Intin Pont. Gotebe Mjorkshian (IMON) Workshup & INGA 20 dis., Jun. 2021, pp. 1–7.
- [26] D. Barbt@nnlt Erräggkossi Shd IM adgotithms: A variationin approach to infestination makinhization, ion depends in Withah Infebrualised Storiesting Systembrd 6 p. Proceeditings of thes 200 in Conference, 7 volude, 2pp p0 14 208.
- [22] H.30ballelo.2020o, I. Frosio, and J. Kautz, "Loss functions for image [7] restofthioniwith neural networks?". IEEE/Edin Metallian Month International
- [7] Pestfranontiwith nisural methods: [Eleipsistin suction stinn Computational] Budging, Gol Féttppeid7-end, Mar. 20 Poor, "Context-aware security
- [23] Av KfiGhewskyletiseaffiling multi ple lphensi of lfelatures from titry, "m2gest", kinkiers2t/0 bf/T5666to, Tech. Rep., 2009.

- [28] DIP. Kingfinti and L. BeBaccadaris: Al methodefor stoch Esticophinizations," 2005 International Conference and contentration of the CLR of Sunthermodule adversaries," IEEE Wireless Comm. Lett., vol. 11, no. 4, pp. 856–860, Apr. 2022.
- M. Letafati, H. Behroozi, B. H. Khalaj, and E. A. Jorswieck, "Deep learning for hardware-impaired wireless secret key generation with man-in-the-middle attacks," 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, Dec. 2021, pp. 1–6.
- [10] E. Bourtsoulatze, D. Burth Kurka, and D. Gündüz, "Deep joint source-channel coding for wireless image transmission," IEEE Trans. Cogn. Comm. Netw., vol. 5, no. 3, pp. 567–579, Sep. 2019.
- [11] D. B. Kurka and D. Gündüz, "Bandwidth-agile image transmission with deep joint source-channel coding," IEEE Trans. Wireless Comm., vol. 20, no. 12, pp. 8081–8095, Dec. 2021.
- [12] M. Letafati, H. Behroozi, B. H. Khalaj, and E. A. Jorswieck, "Wireless-powered cooperative key generation for e-health: A reservoir learning approach," 2022 IEEE 95th Vehicular Technology Conference (VTC-Spring), Helsinki, Finland, Jun. 2022, pp. 1–7.
- [13] K. -L. Besser, P. -H. Lin, C. R. Janda, and E. A. Jorswieck, "Wiretap code design by neural network autoencoders," IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 3374–3386, Oct. 2019.
- [14] R. Fritschek, R. F. Schaefer, and G. Wunder, "Deep learning for channel coding via neural mutual information estimation," in Proc. 20th Int. Workshop Sig. Proc. Adv. Wireless Comm., pp. 1–5, July 2019.
- [15] R. Fritschek, R. F. Schaefer, and G. Wunder, "Deep learning based wiretap coding via mutual information estimation," in Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning (WiseML'20), NY, USA, Jul. 2020, pp.

- Diego, May 2015, pp. 1-13.
- [16] T. Marchioro, N. Laurenti, and D. Gündüz, "Adversarial networks for secure wireless communications," IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP), Barcelona, Spain, 2020, pp. 8748–8752.
- [17] E. Erdemir, P. L. Dragotti and D. Gündüz, "Privacy-aware communication over a wiretap channel with generative networks," IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP), Marina Bay Sands, Singapore, May 2022, pp. 2989–2993.
- [18] D. B. Kurka and D. Gündüz, "DeepJSCC-f: Deep joint sourcechannel coding of images with feedback," IEEE Journal on Selected Areas in Information Theory, vol. 1, no. 1, pp. 178–193, May 2020.
- [19] R. Polikar, "Bootstrap-inspired techniques in computational intelligence," IEEE Signal Process. Mag., vol. 24, no. 4, pp. 59-72, 2007.
- [20] A. Makhdoumi, S. Salamatian, N. Fawaz, and M. Médard, "From the information bottleneck to the privacy funnel," in Proc. of IEEE Information Theory Workshop (ITW), 2014.
- [21] D. Barber and F. Agakov, "The IM algorithm: A variational approach to information maximization," Advances in Neural Information Processing Systems 16: Proceedings of the 2003 Conference, vol. 16, pp. 201–208.
- [22] H. Zhao, O. Gallo, I. Frosio, and J. Kautz, "Loss functions for image restoration with neural networks," IEEE Transactions on Computational Imaging, vol. 3, pp. 47–57, Mar. 2017.
- [23] A. Krizhevsky, "Learning multiple layers of features from tiny images," University of Toronto, Tech. Rep., 2009.
- [24] D.P. Kingma and L.J. Ba, "Adam: A method for stochastic optimization," 2015 International Conference on Learning Representations (ICLR), San Diego, May 2015, pp. 1–13.