Using video scalability for designing safe multimedia transactions

Fabio Piva and Vanessa Testoni
Samsung Research Institute Brazil
Advanced Technology group, Mobile Computing department
Campinas, Brazil
Email: fabiopiva@protonmail.com, vanessa.t@samsung.com

***Abstract*—In this paper we address video-on-demand (VOD) scenarios. Initially, we discuss how previous results on the unsuitability of the current adopted business model for the e-commerce of digital items affects VOD services. Then, we propose a reversible degradation method in order to address the lack of an accurate item validation step in current e-commerce implementations, thus providing robustness against mistaken purchases; the proposed method exploits the Scalable Video Coding (SVC) extension of the H.264/AVC standard. Finally, we illustrate how the proposed validation method can be used as a component for fair exchange protocol design, with the purpose of enabling unambiguous dispute resolution for unsatisfied buyers.**

***Keywords*-Scalable video coding; VOD; item validation; fair exchange protocols; reversible degradation.**

I. Introduction

The increasing widespread access to cheaper broadband connections has been followed by an also increasing interest in video-on-demand (VOD) services among the general public. As a consequence, service providers have emerged in order to satisfy consumers' demand for conveniently-delivered movies through the network in a variety of ways (streaming or downloadable), qualities (high-definition, bandwidth-friendly, etc) and plans (monthly subscriptions, pay-per-access, renting or buying, etc).

In pay-per-access scenarios (such as the service offered by Amazon.com and iTunes Store, for instance), specifically, the purchase protocol usually follows the same sequence of events: First, the user searches for the movie he intends to buy. Then he checks the descriptions of the returned results and, if he is satisfied with any particular instance, places an order for that item – and pays for it. Finally, and only after the payment has been processed by the provider, the content becomes available so that the buyer can access it. This is essentially the same sales model as the one employed by digital music providers (which in many cases also offers VOD content) and, since both types of content are hard to describe univocally, can lead to the same unsatisfactory (i.e., unfair) transaction outcomes as previous research has identified in digital audio e-commerce scenarios [1], [2], [3].

Specifically, due to the digital nature of the products being commercialized, return policies often do not apply in such scenarios [4]. Therefore, ensuring successful outcomes for buy-and-sell transactions becomes a priority, since reverting the transaction is usually not an option.

Much research has been done on how to enhance e-commerce systems with robustness against mistaken purchases. Fair exchange protocols [5], [6], [7], for instance, constitute a class of cryptographic protocols designed with the purpose of allowing mistrusting parties to exchange digital items in an atomic fashion; an exchange protocol is called *fair* if, at the end of the exchange, either both parties obtain their desired items, or none of them does [5]. However, recent results on fair exchange protocols research has shown that, arguably, most previous proposals hold little practical application in real e-commerce scenarios – mainly due to the inherent complexity of currently-available digital items and to the different expectations that each consumer might have towards a particular item [1], [2].

This issue – namely, the *problem of item validation* [1], [2] – arises from the very same way that such protocols are often designed: by treating the digital items as generic sequences of bits, designers tend to neglect item-specific aspects (as well as the way users interact with those items), thus potentially introducing points-of-failure in the protocol – which may ultimately affect the outcome of each transaction [2], [3].

For that reason, recent approaches on this matter have focused on proposing alternative techniques that can enable protocol designers to address such real-world issues. One of such approaches, namely *reversible degradation* [2], [3], [8], aims at enhancing the item validation step of fair exchange protocols by allowing a degraded (i.e., lower quality) version of the item to be delivered to the buyer, for the purpose of evaluation, before any payment is made. The degraded version allows the user to "try out" the product, by checking whether whatever relevant desirable features are present, and to make a better-informed decision about the content he is about to acquire; if this version is satisfactory, the user then pays for a restoring key that, in a software-aided fashion, is able to convert the degraded version into a full-quality item – thus effectively reducing the odds of a non-satisfactory purchase, even in problematic scenarios where indescribable items (such as is the case with multimedia content [1]) are concerned. Notice that the use of reversible degradation does not have to necessarily replace the description-based model – it can enhance it by adding an extra layer of validation to the

protocol.

Similar approaches to reversible degradation have been proposed in the past for video applications. Partial encryption techniques [9], [10] may sometimes preserve certain semantic aspects of the original information; their purpose, however, is mainly to reduce the computational effort required by encryption, so that it can be performed in real time without service interruption – such as is the case with protected streaming, in which preserving the encrypted content's confidentiality is still a goal. Transparent encryption techniques [11], on the other hand, are used in scenarios in which the content needs to be stored securely, but also needs to be easily accessible for secondary operations (i.e., database queries, metadata extraction) without requiring it to be unencrypted;

With all these challenges in mind, we propose a reversible degradation instance which combines the scalable video coding (SVC) extension of the H.264/AVC standard [12] and the Advanced Encryption Standard (AES) specification [13]. Our method can be combined with fair exchange protocols in order to enable suitable item validation for video content. We believe that the current digital content industry could benefit from alternatives that provide a reliable electronic commerce platform, capable of both preserving providers' financial gains and guaranteeing buyers' satisfaction regarding the purchase of digital content.

The remainder of this document is organized as follows: Section II briefly presents related work relevant to our discussion. In Section III, we describe in details our proposed reversible degradation technique, including degradation, key generation and recovery methods, as well as relevant considerations. We conclude in Section V with some final remarks.

II. Related previous work

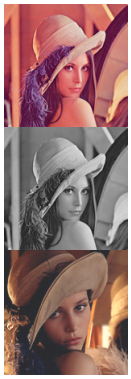
A. The problem of item validation and e-commerce unfairness

Optimistic fair exchange protocols [5] usually follow a common sequence of events: Let us suppose that two parties P and Q are willing to exchange two generic items i_P and i_Q. A common scenario requirement is that P and Q know beforehand the descriptions $desc(i_Q)$ and $desc(i_P)$, respectively, of their expected items; there must also be a publicly-available function $validate(i,d)$ which takes an item i and a description d and returns $TRUE$, if d accurately describes i, or $FALSE$ otherwise.

Therefore, the availability of both a function $validate()$ and accurate descriptions of the items are essential to ensure fairness in this type of protocol. However, for some particular items (i.e., *indescribable items*), providing an accurate description can be a hard task [1], [2]. Such items include, but are not limited to, pictures, digital music, and digital movies. These items are often too complex and can be offered in multiple slightly different versions. When multiple similar, yet non-identical versions of an item are available for purchase on an online provider catalog, the offered descriptions can often fail to include all the information necessary to allow a potential buyer to distinguish between two different versions of the same content. Figure 1(a) illustrates a hypothetical description of an item, which can be satisfied by any of the three similar items shown in Figure 1(b). One should notice that, regardless of what are the expectations of a hypothetical buyer regarding the product he is about to receive after validating $desc(i)$, any of the items i, i' and i'' are eligible for delivery by the provider.

- *Item Summary:* Portrait of model Lena Söderberg
- *Keywords:* hat, bust, plumes, portrait
- *File Specs:* PNG image (bitmap), 256x256 resolution

(a) Description $desc(i)$



(b) Items i, i' and i'', with $desc(i) = desc(i') = desc(i'')$

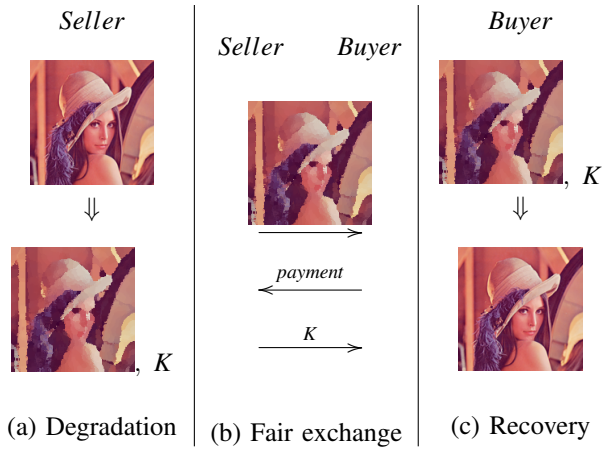
Figure 1: Non-univocal description of indescribable items.

Not only online commercial transactions regarding image items, but also those concerning digital music or movies, for instance, could lead to unfair outcomes caused by indescribability issues. A particular song can be offered in several different versions and a movie can be offered in its original theatrical release or director's cut version, for instance. Rather than being a theoretical problem, this is an observable fact that results in too many customer public complaints that can lead to the discouragement of buyers in engaging in online transactions.

B. Reversible degradation

Reversible degradation [2], [3], [8] was proposed as a solution for enabling robust item validation of indescribable items in fair exchange protocols. The idea is to transform an item in such a way that it becomes clearly deteriorated (aka, *degraded*), but without depriving it from its main functional characteristics [2]. This allows the owner of such an item to release it to the interested counterpart before payment is made, in order to enhance the chances of an accurate validation. If the buyer is satisfied with the validation performed over the degraded version of the item, he then pays for a key K that reverts the degradation process and recovers the item to its full, original quality – as illustrated in Figure 2.

In order for a method to be considered a valid reversible degradation instantiation, several properties must be satisfied [2], [3], [8]. One of these properties states that the buyer must receive a degraded version of the item he is buying, but the degradation can not prevent the item to be recognized and validated – thus effectively binding together the validation artifact (which the piece of information used by the buyer for deciding whether he should proceed with payment or not, i.e. the degraded version) and the item itself. Once the degraded



(a) Degradation (b) Fair exchange (c) Recovery

Figure 2: Reversible degradation concept.

version is acquired, only the restoring key – which is to be delivered by the seller, once payment is made – is needed by the buyer in order to obtain the desired full-quality version.

We note that, from a fair exchange perspective, it is not acceptable that the seller sends low-quality video for validation, and a second, full-quality video after payment is received – since the necessary atomicity of the validation step would be violated. All the information required to have access to the full-quality version must already be in possession of the buyer, except for the restoring key. This is an critical aspect of fair exchange since, after having received the payment, a malicious seller could otherwise send a "full-quality" video that is completely unrelated to the validated low-quality one. Figure 3 illustrates this problem.

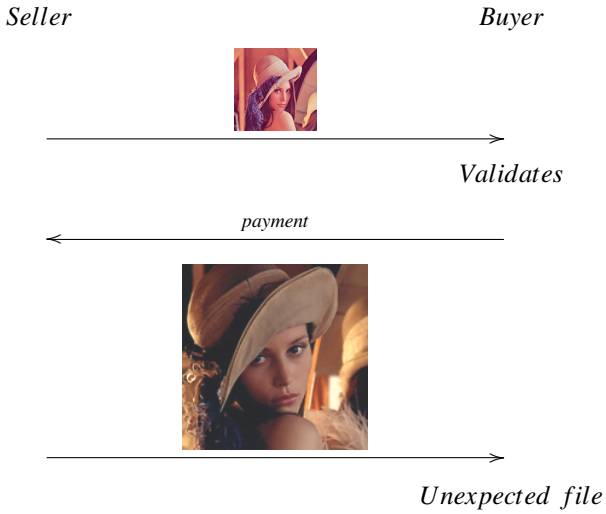


Figure 3: If the validation artifact is not linked to the digital item, undesired outcomes may still occur on the buyer side.

III. A REVERSIBLE DEGRADATION INSTANCE SUITABLE FOR VIDEO CONTENT

In this section our proposed reversible degradation method is described, as well as how it can be implemented on an application level.

A. Item description

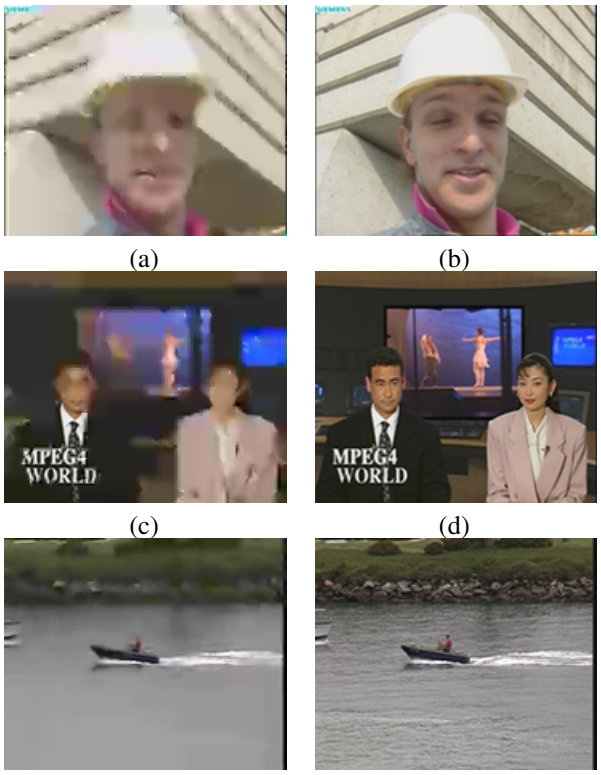
Our proposed implementation of reversible degradation of video content relies on scalability. A video bitstream is called scalable when parts of the stream can be removed in such a way that the resulting sub-bitstream consists of another valid bitstream for some target decoder. The sub-bitstream represents the source content with lower reconstruction quality than that of the complete original video bitstream. Bitstreams that do not provide this property are referred to as single-layer bitstreams.

Scalable bitstreams can be obtained with the scalable video coding (SVC) [14] extension of the H.264/AVC standard [12]. The scalable bitstream can be generated with a *base layer*, which is compatible with H.264/AVC, and several additional *enhancement layers*. By exploiting SVC possibilities, the seller becomes able to generate the base layer with the desired quality and provide it to the buyer as the degraded version of the video sequence item.

Figures 4(a), 4(c) and 4(e) show degraded versions for one frame of the well-known video sequences *Foreman*, *News*, and *Coastguard*, respectively. All these sequences have 176×144 resolution and 24 frames per second (fps). The degraded versions were generated by employing quality scalability and decoding only the base layer. The full-quality versions are shown in Figures 4(b), 4(d) and 4(f), and were generated by decoding all layers of the quality-scalable bitstreams. It can be noticed that, even though the images in Figures 4(a), 4(c) and 4(e) are highly degraded, it is still possible to recognize the video contents – thus allowing the buyer to perform item validation.

All images in Figure 4 were generated with version 9.19.15 of the Joint Scalable Video Model (JSVM) software [15], which is the reference software for SVC. For the quality scalability configuration, we chose the coarse-grain quality scalability (CGS) mode. In this mode, each layer uses the reconstructed frame from the layer below as prediction reference, and is coded by a progressively-lower quantization parameter (QP). The scalable bitstream was generated with only two layers – one base layer and one enhancement layer – and the enhancement layer was encoded with a QP approximately five times lower than the base layer QP for each frame. The group of pictures (GOP) size is 16 frames and the chosen hierarchical GOP structure is shown in Figure 5.

As shown in Figure 5, SVC employs the concept of hierarchical B-pictures [16]. Therefore, temporal scalability can be easily achieved by decoding the desired temporal layer T_i. For instance, every sixteen frames will be skipped if only temporal layer T_0, represented in blue in Figure 5, is decoded. On the other hand, any frame will be skipped if the temporal layer T_4



(a) (b) (c) (d) (e) (f)

Figure 4: Frames extracted from the *Foreman* (a – b), *News* (c – d) and *Coastguard* (e – f) sequences, respectively; (a), (c) and (e) represent degraded versions (i.e., base layer-only decoding), while (b), (d) and (f) represent the full-quality versions.

is decoded, since each temporal layer also includes the frames from the previous layers.

For rate-distortion evaluation purposes, Table I shows results in terms of Y-PSNR versus bitrates, for the encoded *Foreman* sequence. Since the original sequence has a frame rate of 24 fps, the last row corresponds to the decoding of the sequence without any skipped frames and produces the visual results seen in Figure 4(b).

The frames shown in Figures 4(a), 4(c) and 4(e) have, on average, a quality as low as 28.74 dB, 27.13 dB, and 26.65 dB,

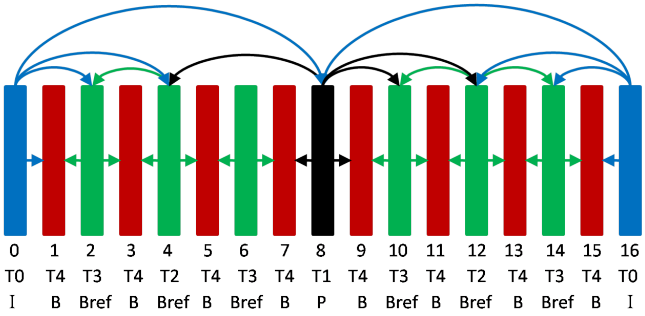


Figure 5: Applied hierarchical B-picture prediction structure.

Temporal layer	Frames per second (fps)	Only base layer		Base + enhanc. layer	
		Bits per second (bps)	Y-PSNR [dB]	Bits per second (bps)	Y-PSNR [dB]
T_0	1.5	19.42	25.53	233.11	55.97
T_1	3.0	33.56	26.46	444.54	54.34
T_2	6.0	50.03	27.63	771.00	53.01
T_3	12.0	66.52	28.33	1258.40	51.96
T_4	24.0	82.96	28.74	2008.04	51.20

Table I: Rate-distortion results for the *Foreman* video sequence. Y-PSNR versus bitrates comparisons vary according to the temporal (T_0 to T_4) and quality layers decoded (only base layer or base layer plus enhancement layer).

respectively – while the frames shown in Figures 4(b), 4(d) and 4(f) have, also on average, a quality as high as 51.20 dB, 51.72 dB, and 50.99 dB, respectively. As expected, the achieved bitrates with the decoding of both base and enhancement layers are much higher than the ones achieved only with the decoding of the base layer.

It is important to note that the parameters for the JSVM software (such as the number of enhancement layers, QPs, GOP size, and scalability mode), can be changed by the seller. Therefore, the results shown in Table I are relative not only to the video content, but also to the seller's choices. A high resolution video sequence could be encoded by combining both quality and spatial scalability modes, for instance – thus resulting in a decoded base layer that would be a blurred, low resolution version of the full-quality and full-resolution video sequence. Another interesting possibility for the seller would be to add temporal scalability in a video sequence with low motion content; in this case, the seller can choose the number of frames to be skipped by decoding the appropriate temporal layer.

B. Implementing reversible degradation with enhancement layer encryption

Security is an essential property of any practical reversible degradation instantiation: recovery of the full-quality item from the degraded version should be easy to perform, provided that the key is known, but otherwise hard to accomplish [2]. Also, and as illustrated in Figure 2, only key K is to be delivered to the buyer once payment is made – which means that the degraded version itself should already contain most of the data from the original (i.e., full quality) item.

Therefore, in order to prevent the buyer from gaining access to the full-quality item before payment, the seller is required to generate the degraded version of the item as a scalable bitstream with a base layer and one single enhancement layer. The former is always accessible, at the buyer side, and represents the low-quality content to be decoded and validated – while the latter is encrypted and, as such, inaccessible (i.e., not decodable) at first.

Another interesting aspect of the proposed method is that, since the recovery process is able to restore the degraded

copy into the exact same bitstream as the original content (provided that the correct K is known), it does not exclude the usage of other-purpose methods in any way. Instead, the degradation process could be, for instance, applied to previously watermarked or DRM-embedded content. Upon reversing the process, the buyer would not only restore the content's full quality, but also any digital artifact intended for controlling unauthorized distribution – or any other purpose, for that matter.

For our proof-of-concept implementation, we relied on the Advanced Encryption Standard (AES) [13], with CBC block cipher mode of operation and PKCS #7 for padding (when needed) in the last block [17]. Our method generates a degraded version of the item by simply stripping the enhancement layer from the original video content, generating a random encryption key K with appropriate (i.e., settable) size[1] and dividing it into 128-bit-sized blocks of data – which are then encrypted under key K and re-inserted into the degraded version; Figure 6 illustrates this initial naive approach. Since AES is a symmetric cipher, the encryption key K is also the decryption key and, therefore, the restoring key for the degradation process.

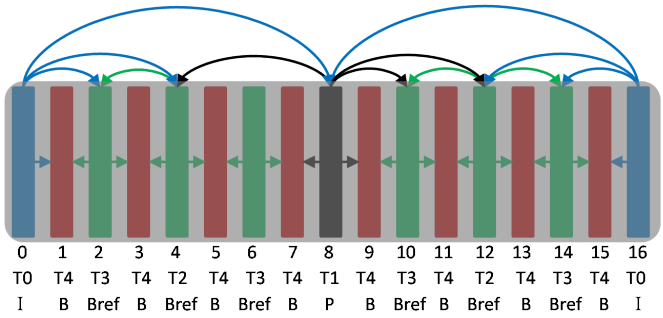


Figure 6: *Naive* approach - all frames have enhancement layer bits encrypted with AES.

If the degraded version indeed refers to the item desired by the buyer, he will complete the transaction by paying for the key. Upon receiving the payment, the seller sends the decryption/restoring key K to the buyer and the enhancement layer can be decrypted – thus allowing the original, full-quality video sequence to be re-generated and concluding the purchase transaction.

We proceed with an analysis of the amount of enhancement layer bits that should be encrypted with AES taking into account the chosen hierarchical structure shown in Figure 5. Table II shows in the second column the scalable coded file sizes in bits for 70 frames of the *Coastguard*, *Foreman*, and *News* video sequences. One can see that for the *Coastguard* sequence, for instance, the coded file size is around 7.5Mb, while for the *News* sequence, the coded file size is about half of bits, only 4Mb. The reason for this difference is because, even though both sequences have the same resolution, frames number and frames per second, the *Coastguard* sequence presents much more scene changes and details than the *News* sequence.

One can also see in Table II that the enhancement bits compose most of the scalable bitstreams, around 97% for the *Coastguard* and *Foreman* sequences and 81% for the *News* sequence. Since the *News* sequence is smoother than the others, its scalable bitstream contains more base layer bits and less enhancement, or details, bits when compared to the other two video sequences.

Video	**All layers [# bits]**	**Only enhancement [bits distribution]**			
(1)	7,567,232	7,415,128 (96.84%)	I	T_0	10.07%
			P	T_1	10.22%
			B_{ref}	T_2,T_3	40.28%
			$B_{non-ref}$	T_4	39.43%
(2)	5,863,464	5,664,272 (96.60%)	I	T_0	12.58%
			P	T_1	11.27%
			B_{ref}	T_2,T_3	39.61%
			$B_{non-ref}$	T_4	36.55%
(3)	4,036,800	3,281,064 (81.27%)	I	T_0	17.75%
			P	T_1	15.10%
			B_{ref}	T_2,T_3	40.92%
			$B_{non-ref}$	T_4	26.22%

Table II: Scalable coded file sizes in bits for 70 frames of the *Coastguard* (1), *Foreman* (2), and *News* (3) video sequences. As expected, the enhancement layer bits compose most of the scalable bistreams for all the sequences. The bits distribution among the Is, Ps and Bs frames of the enhancement layers is also shown.

Considering this analysis, the initial proposal of encrypting all the enhancement layer bits with AES actually requires encrypting always more than 80% of the bits in the scalable bitstream, which can be very inefficient; this approach has been previously proposed [11]. In our context of application, however, we could take advantage of the scalable hierarchical structure: since non-reference B frames, shown in red, are not used for coding/decoding other frames in the sequence but are totally dependent on them, it is not necessary to encrypt non-reference B frames; we illustrate this slightly improved approach in Figure 7. One can see in Table II that these bits composed almost to 40% of the enhancement bits in the sequences *Coastguard* and *Foreman* and around 26% in the sequence *News*. Therefore, 35% of the bits, on average, would be saved from the AES encryption with this optimized approach.

Yet another encryption approach could consider that since all the frames in the GOP of the hierarchical structure depend on the I frame, if only the enhancement bits of this frame are encrypted with AES, all the other fifteen frames in the GOP are protected. One can see in Table II that the enhancement bits belonging to the I frames correspond only to around 10%,

[1]The standard AES specification allows three key sizes (128, 192 or 256 bits, respectively).

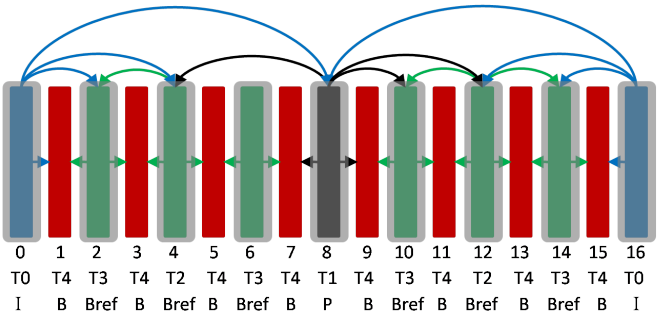


Figure 7: *Optimized* approach - only reference frames, highlighted in gray, have enhancement layer bits encrypted with AES.

13% and 18% of the enhancement layer bits of the sequences *Coastguard*, *Foreman*, and *News*, respectively. Therefore, this is the most efficient approach proposed for the encryption of the enhancement layer bits with AES, without compromising the method security; it is illustrated in Figure 8.

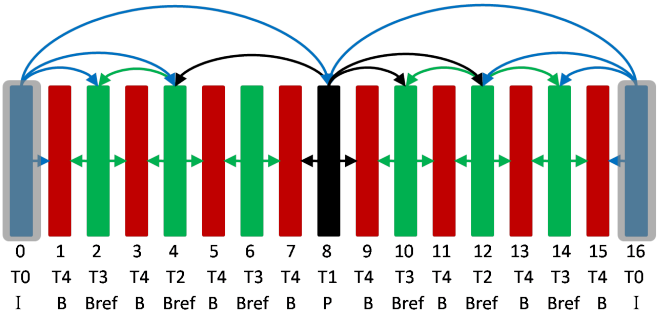


Figure 8: *Best* approach - only I frames, highlighted in gray, have enhancement layer bits encrypted with AES.

IV. An example of fair exchange protocol with semantics-preserving item validation step

Since fairness can only be guaranteed when an accurate item validation step is available for the buyer [5], [7], fair exchange protocols that make it into real-world applications are scarce – mainly because previously published examples are often designed under generic assumptions that do not reflect specific item characteristics and user behavior. A reversible degradation protocol for multimedia content has been proposed in [18]; in this section, we revisit that protocol with the purpose of illustrating how the method described method should be employed in the transaction, in order to improve the accuracy of item validation by preserving the semantic aspects of the desired product. The protocol is illustrated in Figure 9.

Here, we assume that the buyer has already searched the seller's website for the content he desires to purchase, and believes it to be indescribable item i_Q. Also, ID_{i_Q} is the product number that identifies i_Q in Q's system. Finally, *Trans_Num* stands for a transaction label that uniquely identifies this transaction.

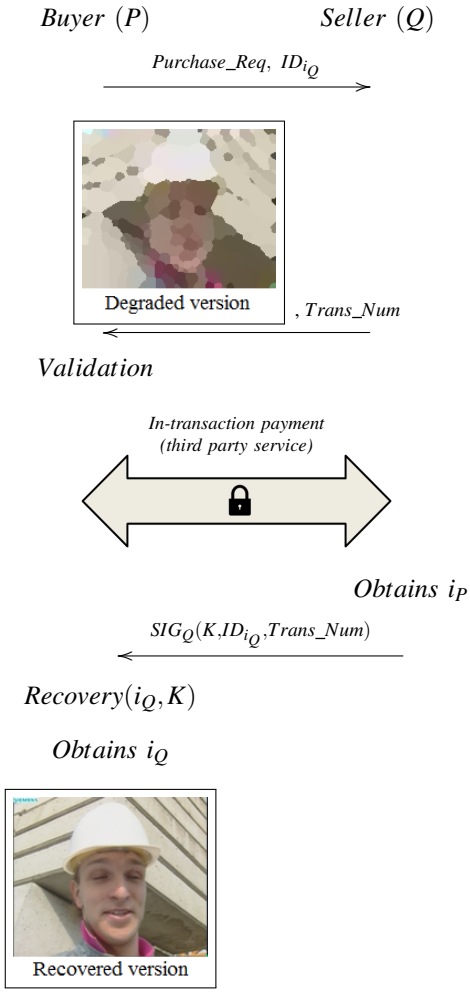


Figure 9: Example fair exchange protocol with semantics-preserving item validation step.

In particular, the use of reversible degradation in this protocol allows the buyer to obtain a sufficiently degraded (i.e., worthless), but still fully-playable version of i_Q before payment – which he can then listen to in order to make sure i_Q is in fact the product he intends to pay for. If it is, the buyer proceeds with the protocol by paying for the recovering key K that will be used as input, together with the degraded version of i_Q, in the recovery process that restores i_Q to its full original quality.

If the degraded version brings the buyer to realize, however, that i_Q is not in fact the product he desires, he can simply abort the protocol without paying for (and thus without obtaining) K – which ensures fairness for the buyer. Because the full quality version of i_Q cannot be obtained from the degraded version without K, seller's fairness is also guaranteed. Exceptional outcomes for the transaction would include, for instance, situations in which $K' \neq K$ is delivered after payment – which would prevent the buyer from successfully recovering i_Q; but even in this scenario, dispute resolution would be simple to

accomplish (since no "wrong product" – only a wrong key – had been delivered, no issues concerning no-return policies apply; the judge would be able to settle the situation either by demanding the correct K from seller, or by revoking i_P).

V. Conclusion

In this work, we proposed a solution to the problem of fairly exchanging (i.e., trading) video content. By taking into account semantic aspects of information, we were able to circumvent the inherent indescribability of multimedia items that, in the current description-based model, prevents accurate item validation and may lead to unfair outcomes. Our method implements the concept of reversible degradation, which we achieve by employing the scalable video coding (SVC) extension of the H.264/AVC standard and the AES encryption algorithm to generate degraded versions of video sequences. After the buyer receives the degraded version of the candidate video for purchase, he then validates that version and sends the payment – upon which the seller sends the restoring key K and the full-quality video sequence can be recovered, without the need of re-downloading the content.

Our contribution improves on previous approaches on trading digital products by taking into account both fair exchange and consumer needs; it enables accurate item validation, thus allowing the potential buyer to verify the candidate product before any payment is made. This fact alone enhances quality-of-service, in comparison to traditional models, by reducing buyer-side risk and, as a consequence, increasing trust on the transaction. As for seller-side protection, the proposed technique relies on state-of-the-art cryptographic artifacts, and is flexible enough to enable several levels and modes of reversible degradation. Therefore, the seller can, in a simple and software-aided fashion, configure the technique according to the video content and to the quality of service he desires to provide.

In order to illustrate the use of the technique, we have implemented a proof of concept composed by the server application at the seller side and by the client at the buyer side. The seller application, *SafeCine*, enables the seller to vary the degradation level of each video item independently; the buyer application effectively runs on a tablet. A brief video illustrating the basic functions of our proof of concept is available at [19].

As a final note, we state that, in order to allow for a less ambiguous dispute resolution – which is required in the case of an unsuccessful outcome [5], [7] – the purchase protocol might benefit of further binding the key to the sold content; this can be accomplished, for instance, by specifying the final message as a cryptographic signature of K and the cryptographic hash of the degraded version – thus introducing not only fairness to the transaction, but also non-repudiation, in a similar fashion to previous approaches to reversible degradation for other types of content.

As future work, user evaluation remains our priority; we shall design and conduct experiments focusing on how our method compares to traditional approaches regarding mistaken purchases prevention, and how it impacts the user in the task of choosing a product. Also, we intend to explore the possibilities of the recent Scalable High Efficiency Video Coding (SHVC) [20], which is the scalable extension of the state-of-the-art standard High Efficiency Video Coding (HEVC).

References

[1] A. Bottoni, G. Dini, and T. Stabell-Kulø, "A methodology for verification of digital items in fair exchange protocols with active trustee," *Electronic Commerce Research*, vol. 7, no. 2, 2007.

[2] F. R. Piva and R. Dahab, "E-commerce and fair exchange: The problem of item validation," in *International Conference on Security and Cryptography (SECRYPT)*. Seville, Spain: SciTePress Digital Library, 2011, pp. 317–324.

[3] F. Piva and R. Dahab, "E-commerce of digital items and the problem of item validation: introducing the concept of reversible degradation," *Applicable Algebra in Engineering, Communication and Computing*, vol. 24, no. 3-4, pp. 277–308, 2013.

[4] Amazon Legal Department, "Amazon Music Terms of Use," Section 1, Item 1.1. Updated on Jun. 2014. [Online]. Available: goo.gl/VwjfUU

[5] N. Asokan, "Fairness in electronic commerce," Ph.D. thesis, University of Waterloo, Waterloo, Canada, Jan. 1998.

[6] I. Ray, "Fair exchange in e-commerce," *ACM SIGecom Exchanges*, vol. 3, no. 2, pp. 9–17, 2002.

[7] H. Pagnia, H. Vogt, and F. Gartner, "Fair exchange," *The Computer Journal*, vol. 46, no. 1, pp. 55–75, Jan. 2003.

[8] F. Piva, "Addressing human factors in the design of cryptographic solutions: a two-case study in item validation and authentication," Ph.D. thesis, University of Campinas, Institute of Computing, Campinas, Brazil, Mar. 2014.

[9] T. Kunkelmann and U. Horn, "Video encryption based on data partitioning and scalable coding – a comparison," in *Interactive Distributed Multimedia Systems and Telecommunication Services*, ser. Lecture Notes in Computer Science, vol. 1483, pp. 95–106. Springer Berlin Heidelberg, 1998.

[10] H. Cheng and X. Li, "Partial encryption of compressed images and videos," *Signal Processing, IEEE Transactions on*, vol. 48, no. 8, pp. 2439–2451, Aug 2000.

[11] J. Dittmann and A. Steinmetz, "Enabling technology for the trading of mpeg-encoded video," in *Information Security and Privacy*, ser. Lecture Notes in Computer Science, vol. 1270, pp. 314–324. Springer Berlin Heidelberg, 1997.

[12] H. Schwarz, D. Marpe, and T. Wiegand, "Overview of the scalable video coding extension of the H. 264/AVC standard," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 17, no. 9, pp. 1103–1120, 2007.

[13] J. Daemen and V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard*. Springer, 2002.

[14] C. A. Segall and G. J. Sullivan, "Spatial scalability within the H.264/AVC scalable video coding extension," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 17, no. 9, pp. 1121–1135, 2007.

[15] "Joint Scalable Video Model (JSVM) Version 9.19.15," *(JVT)*, 2011.

[16] H. Schwarz, D. Marpe, and T. Wiegand, "Hierarchical B pictures," *Joint Video Team (JVT)*, 2005.

[17] B. Kaliski, "PKCS #7: Cryptographic Message Syntax Version 1.5," RFC 2315 (Informational), Mar. 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2315.txt

[18] F. Piva and R. Dahab, "Modern fair exchange protocol design: Dealing with complex digital items," in *XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)*, Manaus/Brazil, 2013.

[19] A. I. Authors, "Reversible degradation for video content: a proof-of-concept demo," Apr. 2015. [Online]. Available: https://www.dropbox.com/s/3zvtsom1vqff46u/Video.zip?dl=0

[20] J. Chen, J. Boyce, Y. Ye, and M. Hannuksela, "Scalable high efficiency video coding draft 4," *Joint Collaborative Team on Video Coding (JCT-VC)*, 2013.