New Exchange Model for Child Pornography Analysis

Ruud Verbij
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
cp@ruudverbij.nl

ABSTRACT
This research concentrates around the topic of the criminal exchange of child pornography material on the Internet. The existing scientific material on this criminal exchange lacks technical details that could help police detectives work more efficiently in child pornography cases. This paper specifies a new criminal exchange model of child pornography that describes (1) the current child pornography user behavior and (2) the new Internet based communication media and anonymization techniques used by child pornography offenders. The specified criminal exchange model has been evaluated and verified by interviewing police detectives concerned with online child pornography cases.

Keywords
child pornography, high tech crime, criminal exchange model

1. INTRODUCTION
With the arrest of Robert M. in December 2010 [1] the Netherlands’ police agency caught, allegedly, the biggest child abuser ever in the Netherlands. On his computer, detectives found (hidden in a partially deleted TrueCrypt folder) eight terabyte containing images and videos of child abuse. Along with the images and videos came the digital equivalent of 64,000 A4 papers containing chat logs with other child abusers, which led to the arrest of numerous of other child abusers in the Netherlands, Norway, Germany, the United States, Australia and many more countries. These arrests led to the question whether current detection methods used by police agencies to catch child abusers are still valid for the new Internet era [28]. The current detection methods are based upon exchange models of child pornography (CP) which may not really be adapted to this new era and therefore they may need to be revised. This research will try to answer the question of how to revise such exchange models to satisfy the need of police detectives for better analysis and detection methods.

Digital CP can be defined in multiple ways, this research will use a definition that is derived from the legal definition given by [11], which cites the PROTECT Act of 2003:

"...it is a crime to possess, manufacture or distribute pornography containing visual depictions of (a) a real child engaging in sexual acts or (b) a digital image, computer image, or computer generated image that is, or is indistinguishable from that of a minor engaged in sexually explicit conduct." from (18 U.S. Code Paragraph 2256(8) (B))

This research acknowledges the legal definition of CP but it is not taking into account the issues related to computer generated images since they need to use different solutions than the ones discussed in the paper. Furthermore, images and videos are widened to encompass digital material, leading to the following CP definition that is used by this research:

Digital child pornography is defined as digital pornography containing visual depictions of a real child engaging in sexual acts or a minor engaged in sexually explicit conduct.

In order to be able to describe the criminal process involved in the distribution, a type of model should be introduced to model the different steps involved in the process. This research will use Crime Schemes as proposed in [31]. Steps in this process follow a flow. This means that certain processes depend on others, which need to be performed first. Groups of processes (categories) belong to each other and together form a category in the simplified model of the crime. In stealing a bike for example, there are different steps in how to break the lock, but they relate to each other and form the ‘breaking the lock’ category in the simplified model. Some different paths exist in breaking the lock, but it is always right to consider that one needs to first break the lock, before removing it from the bike. Since this research investigates exchange models and describes them via crime schemes, such an exchange model will from now on be called a criminal exchange model.

Different authors have suggested that there should be more scientific research into the area of criminal exchange models of CP [28, 32, 27]. They conclude that most of what is known about the exchange of CP is due to successful arrests and that there are exchange methods (involving high tech components) which are not yet found by police detectives. Therefore new research must be conducted to gather more information on these high tech crime components in the exchange of CP which could then be included in the existing criminal exchange models.

The main research question in this research is ‘How can the currently used main criminal exchange models of child...
pornography be adapted to describe (1) the current child pornography user behavior and (2) the new Internet based communication media and anonymization techniques used by child pornography offenders?’. This main research question is divided into three different sub questions:

1. What are the currently used main criminal exchange models of CP?
2. What are the main differences between the communication media used in the past and today in the exchange of CP?
3. How can the changes associated with the current CP user behavior and the new Internet based communication media be reflected in the currently used main criminal exchange models of CP?

The research questions (1) and (2) are answered using a literature study. Finally, research question (3) is answered by proposing a new CP criminal exchange model and by verifying it using interviews with seven police detectives that are concerned with the recent arrests of several child pornography offenders.

This paper is organized as follows. In Section 2 an overview of the current criminal exchange models of CP is given. Furthermore, this section provides the answer of the research question (1). Section 3 provides the technical enhancements on the CP criminal exchange models, providing the answer to research question (2). In Section 4 a new CP criminal exchange model is proposed, which is verified by interviewing police detectives that are involved with the recent arrests of several child pornography offenders. Moreover, this section answers research question (3). Section 5 concludes and provides recommendations for future work.

2. CHILD PORNOGRAPHY EXCHANGE MODELS

This section provides an overview of the current criminal CP exchange model. Furthermore, this section derives criteria and compares the discussed criminal CP exchange models.

Several papers and books briefly mention the exchange of CP, such as [32, 19, 30], which briefly focus on CP exchange via Internet and, [25, 11], which briefly focus on the CP exchange via usenet, bulletin boards or websites. However, only few of these papers that describe the CP exchange, go into more detail, see e.g. [17, 33, 28, 12]. The description level of detail used by papers is quite different and will therefore be elaborated in different sections.

However, only Faber et al. [17] provides a more complete description of a criminal CP exchange model. The other criminal CP exchange models discussed in this paper are derived by the author of this paper by carefully studying the information contained in the referenced papers and books.

In Table 1 the different criminal CP exchange models are compared. These CP exchange models are compared using the following criteria:

- **Completeness of the criminal exchange model**: this refers to the number of categories modeled by the criminal exchange model. The steps defined in this research, which need to be modeled by a criminal exchange model are:
  - Production: The physical abuse and the recording of it. Also location selection, victim recruiting, editing, lighting, restructuring of the video, etc. fall in this category, since this research is not focused upon this category and only needs a way to model all processes that are not involved in the criminal exchange model.
  - Hiding: Hiding information that could lead to the producer or distributor, by using techniques such as encryption and stenography [21].
  - Distribution: Making CP material available for others to download/view.
  - Downloading: Downloading or streaming CP material.
  - Storage: Storing CP material and possibly hiding it.

In Table 1, the grade ++ represents the situation that all the steps mentioned above are supported, while - - means that none of these steps are supported.

- **Modeling of Anonymity**: this refers to whether the criminal exchange model, models in detail the support of anonymity in the criminal CP process. Anonymity support refers to the support of activities in such a way that the identity of the CP user cannot be detected. In Table 1, the grade ++ represents the situation that a criminal exchange model provides all means to model Anonymity support. The grade - - represents the situation that the criminal exchange model does not provide any means of modeling Anonymity support.

- **Modeling of Distribution types**: this refers to whether the criminal exchange model, models in detail the support of Distribution type in the CP process. Distribution type refers to the way of how the CP media is distributed. In Table 1, the grade ++ represents the situation that a criminal exchange model provides all means to model the Distribution type. The grade - - represents the situation that the criminal exchange model does not provide any means of modeling the Distribution type.

- **Transaction type**: this refers to the type of actions involved within the Criminal CP process. These transactions can be either Financial means (money) or CP interexchange material.

2.1 Faber et al., 2011 [17]

Figure 1 gives the visual representation of the criminal CP exchange model proposed by [17]. This figure shows four different categories (Production, Hiding, Distribution and Storage). [17] groups different steps in the process of the CP exchange. The step Editing is not included in such a group since it is not considered as being an important step in the criminal CP scheme.

Faber et al. [17] is the only research document that describes some sort of criminal exchange model for the criminal process of CP. This criminal CP exchange model [17] describes the process that is sketched in Figure 1. The Editing event is just a video editing event and therefore it can be left out of the exchange model. The different types of steps that could be taken in the Coding event are similar to what other authors have concluded (i.e. [33, 19, 32]). It includes untraceability, invisibility, illegibility and unrecognizability. The Payment event does not only involve
cash payments, but also includes interchange of CP material that is found in several other articles as well (i.e. [33, 28, 32]). The Distribution event only covers the description different communication media such as newsgroups [8], bulletin boards [10], P2P [6], e-mail, IRC [5], FTP [3] and websites, but lacks to clarify the specifics for CP exchange on these communication media or the amount of usage on these different communication media. The authors of [17] make a clear distinction between the exchange via a website (acquire domain, acquire hosting and distribution) and exchange via other media (acquire costumers, payment, distribution). This is in clear contrast with different other papers, [33, 28, 12], which all state that using a website to distribute CP always includes a payment.

Figure 1. Part of the Crime Scheme as proposed by Faber et al. in [17]

The Abuse Recording step is thoroughly described, covering topics as the severity of the recordings [25], but it also covers topics such as the victim selection, grooming, consolidation, staff recruitment and location selection. The Editing step involves the anonymization of the abuse, making scenes, compiling it, making descriptions, etc. The Acquire Domain and Hosting involve the process of getting a website and domain name to spread the material. This can be bought online using (stolen) credit cards, web money or servers that could be hacked. The Acquire Customers event, describes the process of getting customers to find the CP material, in addition to websites, it involves mass mailing and it provides adds on the normal porn websites or getting inside costumers from fora or networks. The Payment event could be either money (using (stolen) credit cards, web money, billing companies) or interchange of CP material. The Distribution process involves the uploading and downloading of the CP material via virtual communities, news groups, fora, p2p, e-mail, chat, FTP and websites. The Storage step involves storing the material and hiding it from authorities and other users of that computer or network.

The processes modeled by Faber et al. involving the abuse and pre-abuse steps are in this research modeled to one process called Abuse Recording, and therefore it is classified into the Production category. The steps modeled in the process Coding are used to hide the producer’s and distributor’s identity and is therefore classified into the Hiding category. The processes that cover the Acquire Customers steps and the steps of leading them to the CP material are grouped together with the actual distribution and payment processes to form the Distribution category. The storage process modeled by Faber et al. is considered to be the Storage category in this research. Faber et al. elaborates thoroughly on the criminal CP exchange model and therefore are rated with a + on the completeness of the criminal model. The model lacks on providing details on modeling the anonymity and the ability to model Anonymity Support is therefore rated with a -. Faber et al. also lacks on providing up-to-date distribution media and is therefore rated with a -. The types of transactions involved are both Money and the Interchange of CP material, see Table 1.

2.2 Wortley et al., 2006 [33]

Figure 2 provides the visual representation of the criminal CP exchange model proposed in [33]. This figure shows three different groups of processes (Production, Distribution and Downloading). Wortley et al. [33] emphasize that recent police activity on different open or semi-closed networks has led most CP users to change their communication means to more closed networks such as closed P2P networks, closed bulletin boards and closed chat rooms instead of websites, e-mail and newsgroups. Similar results are found in [28, 12]. Furthermore, Wortley et al. state that there are hardly any financial interactions involved within the process of distribution since almost all new material is produced by amateurs who do not seek financial gain in their child abuse. This resembles findings by other research activities (i.e., [11, 28]) but it contradicts findings provided by, among others, the UN in 2006 (cited in [28]). The UN stated that global CP exchange made about 6 billion dollar in 2005. Furthermore [30], states that about 50% of all CP users have paid to watch CP. The information provided by [11, 28, 30] show that there is a big market for CP exchange. Wortley et al., [33] lacks to provide the necessary details on the specifics on the different communication media for the CP exchange.

Figure 2. Derived Crime Scheme from Wortley et al. in [33]

The Production process models the production of material, mostly made by amateurs but also covers professional recordings. The Distribution process describes in short the existence of pedophile rings or organized crime groups that interchange the CP material on different platforms like websites, e-mail, instant messages, newsgroups, bulletin boards, chat and p2p. The Downloading process describes the actual search for CP material by CP users. In [33], it is stated that mass mailings and the ads on normal porn websites hardly exist anymore. The process described by Wortley et al. as the Production process is modeled as the Production category. The Distribution process is modeled as the Distribution category and the Downloading process is modeled as the Downloading category.

Wortley et al. do not elaborate thoroughly on the criminal CP exchange model, therefore the completeness of the criminal model is rated with a + / -. The modeling of Anonymity Support is not supported and therefore rated with a -. The ability to model up-to-date distribution media is a little bit better and therefore rated with a -. The type of transactions involved is only the Interchange of CP material, see Table 1.
2.3 Van Wijk et al., 2009 [28]

Figure 3 depicts the visual representation of the criminal exchange model provided by [28]. This figure shows four different groups of processes (Production, Distribution, Downloading and Storage).

Van Wijk et al. [28] describes four different types of distribution; commercial distribution (via mail delivery), commercial websites (pay by credit card or emoney), open networks (open IRC channels, open P2P networks, open bulletin boards) and closed networks (chat, e-mail, closed bulletin boards and closed P2P networks). Due to recent police activity against CP, more or less all distribution belongs to the last category, i.e. closed networks, see [33, 12]. Van Wijk et al. takes a closer look into the high tech components involved in the distribution process. However, the focus is more on the CP downloaders instead of being on the CP distributors. Some of the mentioned high tech components involve (1) virtual hard drives to browse without leaving traces on the computer [9], (2) the use of disk encryption software to hide downloaded material on specific parts of the hard drive [2], (3) the use of proxy servers as storage locations or to browse anonymously [7] and (4) software to erase a hard drive.

![Figure 3. Derived Crime Scheme from Van Wijk et al. in [28]](image)

The process described by Van Wijk et al. as Production is mentioned in the model, but no further information is given about this step. The Distribution step is different from earlier models and elaborates more on the different distribution media. The distribution is split in four different types of distribution.

- **Commercial distribution**: uses post-order to order CP material online and receive it by post mail.
- **Commercial websites**: websites that run on servers mostly located in eastern European cities, which are distributing the CP material by selling it online.
- **Open networks**: networks which can be used to distribute CP material without requiring any password or security protection. Such open networks are: open P2P networks, open chat rooms and open bulletin boards.
- **Closed networks**: networks that can be used to distribute CP material using the same media as the open networks, but which are closed by using password and security protection, such as encryption and decryption.

The Production process is modeled as the Production category. The different distribution media are grouped together as the Distribution category since all these distribution media types involve the characteristics of this category. The Downloading process is modeled as the Downloading category and the Storage process is modeled as the Storage category.

Van Wijk et al. elaborates on the criminal exchange model and the completeness of the criminal model is therefore rated with a +. It also presents some details on the Anonymity support and therefore it is rated with a +. The ability to model up-to-date distribution media is relatively extensive and therefore rated with a +. The types of transactions involved are encompassing both Money and Interchange of CP material, see Table 1.

2.4 Callanan et al., 2009 [12]

Figure 4 depicts the visual representation of the criminal exchange model provided in [12]. This figure shows two different groups of processes (Downloading and Distribution).

Callanan et al. [12] describes different communication media used to distribute CP material than the other CP exchange models described in the previous subsections. In particular, [12] describes Freenet [4] as a way to distribute CP material in encrypted and sliced packets which are then distributed to users of Freenet on a P2P manner (including non CP users). Freenet supports multiple anonymization options, making it possible to easily hide the identity of its users. Furthermore, [12] describes several characteristics of Usenet system and the incentives of why this system is used among CP users. Both these communication media (i.e., Distribution process) have the characteristic that it is really hard to delete the CP material once it has been distributed.

![Figure 4. Derived Crime Scheme from Callanan et al. in [12]](image)

The Hiding Identity process describes different communication media that could be used either by downloaders of distributers for the exchange of CP. The actual downloading process models Anonymity Support by those communication media. The distribution process describes the Anonymity Support offered to distributors of CP material. [12] describes various methods of identity hiding, which in turn could be used for downloading and/or distribution. The Hiding identity process describes different communication media that could be used by either CP material downloaders or CP material distributors. The actual Downloading process encompasses the anonymity support used by those communication media. The Distribution process encompasses the anonymity support offered to distributors of CP material. The Hiding Identity process as modeled by Callanan et al. cannot be classified in any of the categories introduced at the introductory part of this section. In particular, this process encompasses both the identity hiding of CP material downloaders and CP material distributors. The Downloading process is modeled as the Downloading category and the Distribution process is modeled as the Distribution category.

Callanan et al. does not elaborate on the criminal ex-
change model and the completeness of the criminal model is therefore rated with a -. The detailed description of Anonymity support is rated with a +++. The detailed description of up-to-date distribution media is also rated with a ++, since it is very elaborate. The types of transactions involved are not discussed, see Table 1.

2.5 Conclusion
A comparison between the criminal CP exchange models described in this section is depicted in Table 1. The criteria used for this comparison are given in the introductory part of section 2.1. From this table it can be seen that the only detailed criminal CP exchange model is found in [17]. The components of this model are mentioned by other authors as well, except for the lack of payment in distribution via websites, which is not covered in [17]. The amount of usage of different communication media has made a switch from open networks to more closed ones as found by [33, 28]. The types of CP payment methods mentioned in the exchange models differ. Though, it can be stated that the more advanced a CP user is, the less likely he/she will favor paying for CP material. In particular, he/she will be far more interested in interchanging CP material, and thereby becoming more and more important in the online world of CP exchange [28, 25, 21, 17]. [28] describes several high tech components involved in the CP material Downloading process and its Distribution (virtual hard disks, disk encryption software and proxy servers). [12] describes in more detail several communication media types (Usenet and Freenet) and the anonymity support used for the actual CP material distribution. However, [12] is not providing any information on the used transaction types. [17] and [28] use both Money and Interchange of CP material as transaction types, while [33] uses only the interchange of CP material as transaction type.

Table 1. Comparison of current criminal CP exchange models

<table>
<thead>
<tr>
<th>Author</th>
<th>Completeness of the criminal exchange model</th>
<th>Modeling of Anonymity</th>
<th>Modeling of Distribution types</th>
<th>Transaction type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faber et al. [17]</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>Money and interchange</td>
</tr>
<tr>
<td>Worley et al. [33]</td>
<td>+/-</td>
<td>-</td>
<td>-</td>
<td>Interchange</td>
</tr>
<tr>
<td>Van Wijk et al. [28]</td>
<td>+/-.</td>
<td>+</td>
<td>+</td>
<td>Money and interchange</td>
</tr>
<tr>
<td>Callanan et al. [12]</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>Not discussed</td>
</tr>
</tbody>
</table>

3. ENHANCEMENTS OF CP EXCHANGE MODEL COMPONENTS
This section describes the ongoing technical enhancements on the CP criminal exchange models. The technical enhancements that will be discussed in this section will also be rated on the scale that the different criminal exchange models were rated on in Section 2. The results can be found in Table 2.

3.1 The Onion Routing (TOR)
Routing traffic through different hops is a method of anonymizing internet browsing and has been used for several years [24]. In 2004, Dingledine et al. [15] proposed the so called The Onion Routing (TOR) protocol in which traffic is routed through three different hops and is encrypted in such a way that hops along the way can only see the identity of the previous hop as being the sender and the identity of the next hop as being the destination. In other words the intermediate hops cannot see the identity of the sender that created the packet and the identity of the receiver where the generated packet was addressed to. This provides in principle maximum anonymity since hop 1 only knows the sender and hop 2; hop 2 only knows hop 1 and hop 3; hop 3 only knows hop 2 and the final destination. None of the hops are able to know both the sender and the receiver of the internet traffic. Since the encryption standards and security protocols are verified [18] to be secure, if used properly, could provide high anonymity for CP users. Furthermore, TOR provides the so called ‘hidden services’. Hidden services are websites that can only be accessed if their address is known (being a 16 character wide random address). The location of the hidden services remains a secret since accessing the address is provided through a rendezvous point. Connections from the rendezvous point to the sender or receiver are done through TOR (and thus uses at least three hops). Visiting such hidden services is done by connecting to a rendezvous point through TOR (meaning that the rendezvous does not know who the sender is), which then opens a connection to the hidden services through TOR (meaning that hidden services doesn’t know who the rendezvous point is). It could therefore be deduced that both the sender and the hidden service are not able to know the identity of the opponent. This also holds for the rendezvous point. This could stimulate CP users to upload and share CP material using hidden services that are specially designed for CP. In that way distributors and downloaders of CP are considered to be completely anonymous.

TOR is able to support various categories of the CP criminal exchange model, namely Hiding, Distribution, Downloading and Storage. This is rated with a + for the completeness of the criminal exchange model, see Table 2 since Production step is not included in this model. The support of Anonymity and Distribution methods are both graded with a +++, since they can be well provided by the hidden services.

3.2 Freenet
Freenet [13] provides similar features as the hidden services provided by TOR. The exception is that everybody is partly able to share the hidden service. Freenet is a P2P-service which routes and disseminates requests, uploads and downloads among different users in chunks [13]. All chunks are requested through different hops and are therefore spread anonymously. The content is encrypted and chopped into chunks before spread through the network. Freenet can be used in either Darknet mode or Opennet mode, where networks are based upon friends only or on the entire user base, respectively.

Freenet is able to model various categories of the CP criminal exchange model, namely Hiding, Distribution and Downloading. Since rarely requested parts disappear in the network, the Storage category does not apply to Freenet. This is rated with a +/- for the completeness of the criminal exchange model, see Table 2. The Anonymity Support and Distribution methods are well modeled. Therefore
they are rated with a ++.

3.3 Anonymous remailers

Normal email traffic can be subject of investigation since the source address is exposed, leading to loss of anonymity. To regain this level of anonymity, anonymous remailers can be used, see e.g., [14]. In general, they are used to forward an email to someone anonymously by stripping all identifiable information of the email leaving nothing but the bare text and the receiver. Some of these remailers offer additional features such as the ability of two-way communication by storing lists of senders and their email addresses (though, this is hazardous information that is being stored). Since this could still lead to the threat of being discovered by applying traffic analysis, Mixminion remailers can be used [14]. This type of remailers take notion of the traffic analysis characteristics and use multihops to forward emails using e.g., delays and encryption.

Anonymous remailers are able to support the distribution of CP material and the recruitment of costumers for CP websites. Since these processes are only involved in the Distribution, this is graded with a - - for the completeness of the criminal exchange model. Different design techniques of these remailers offer different levels of anonymity; it is often not very clear who runs a remailer and if it has not yet been hacked. It therefore can only get a grade of + for the ability of modeling anonymity. The number of distribution methods is not increased with the introduction of anonymous remailers, though, one of them (email) has been extended, it is therefore rated with a - on the modeling of distribution, see Table 2.

3.4 TrueCrypt

TrueCrypt is an on-the-fly encryption tool that can be used to encrypt either parts or complete harddisks. TrueCrypt uses very strong cryptographic principles [22] by which it can provide strong privacy if strong keys are used. TrueCrypt can thus be used to encrypt parts of the harddisk containing CP material for storage. Furthermore, TrueCrypt offers the option to use hidden volumes within such an encrypted partition. It is very difficult to detect and prove the existence of such a hidden volume, and it therefore provides plausible deniability of that hidden volume. A CP user could for example reveal the body of an encrypted partition which contains somewhat sensitive information, creating the plausible deniability for a hidden volume within the encrypted partition.

Since TrueCrypt only gives the possibility to model Storage, it is rated with a - - on completeness of the exchange model. The plausible deniability makes it possible to rate with a ++ on the ability to model Anonymity Support. TrueCrypt does not provide any support for CP material Distribution and therefore it is rated with a - - on the modeling of Distribution, see Table 2.

3.5 Anonymous credit cards

Paying for CP material has been declining according to some research results [33, 28, 11] since police investigators have been investigating the flow of money to get a hold on downloaders of CP. Due to this fact, CP distributors who were in the business only for financial reasons have disappeared and the transaction type of exchange has been changed to interchange of CP material.

Anonymous credit cards can be used to perform a transaction that involves CP exchange anonymously. These credit cards can be bought using cash and can be used to perform payments online and offline. Furthermore, they can be used to perform transactions from other (anonymous) credit cards or stolen credit cards. This could be used to buy CP material online anonymously, without the possibility of tracing the transaction [29]. Therefore, this can potentially be considered as being a new burst for commercial CP material distributed from countries with a lack of legislation on CP [20].

Anonymous credit cards only enhances the Distribution category and is therefore rated with a - - on the completeness of the exchange model, see Table 2. The anonymity that could possibly be modeled with anonymous credit cards is strong, though, these credit cards infer a few risks when used other than in the CP process. It is therefore rated with a + on the ability to model Anonymity Support. Since only the Payment method is enhanced and not the Distribution methods, the ability to model Distribution is rated with a - -.

3.6 Webcam hacking

There have been reports [23, 26] of viruses that can turn webcams on without that the user of the computer knowing. This could lead to serious problems within the Abuse recording process, e.g. with grooming and consolidation being easier if children are confronted with secretly recorded images or videos.

These Webcam hacks only enhances the Production category and are therefore rated with a - - on the completeness of the exchange model, see Table 2. The anonymity that could possibly be modeled with Webcam hacks is strong and it is rated with a + on the modeling of Anonymity Support. The Distribution modeling is not supported by Webcam hacks and is rated with a - -.

| Technique           | Completeness of the │ Modeling of │ Modeling of Distribution types | Transaction type |
|---------------------|----------------------|-------------|---------------------------------|-----------------|
|                     | model                | Anonymity   |                                 |                 |
| TOR [15]            | ++                   | ++          | ++                              | Not discussed   |
| Freenet [13]        | +/-                  | ++          | ++                              | Not discussed   |
| Anonymous remailers [14] | - -               | +           | -                               | Not discussed   |
| TrueCrypt [22]      | - -                  | ++          | -                               | Not discussed   |
| Anonymous credit cards [29] | - -               | +           | -                               | Money           |
| Webcam hacks [23, 26] | - -                | +           | -                               | Not discussed   |

4. PROPOSED EXCHANGE MODEL

This section proposes a new CP criminal exchange model (Section 4.1 and 4.2) that is verified by the use of interviews with police detectives that are concerned with the recent arrests of several child pornography offenders (Section 4.3).
4.1 Specification
A new criminal CP exchange model should be able to integrate most of the exchange models described in Sections 2 and 3. Since the exchange model proposed by Faber et al. [17] provides the most complete criminal exchange model, it will be used as the main framework, see Figure 1.

Some research results contradicted specific details of actions in the CP exchange model proposed by Faber et al. [25, 21]. Furthermore, [28] proposed to classify the distribution methods into four different categories of distribution. The Downloading category was included in multiple CP exchange models (see Figures 4, 3 and 2) but was not included in Faber et al.’s model. These differences have been added to the original CP exchange model proposed by Faber et al., see Figure 5.

The step that is missing in the CP exchange model of Faber et al. and is strongly supported in other exchange models, e.g., in Callanan et al. [12] TOR and Freenet, is related to Anonymity support. Therefore, the proposed exchange model will enhance the CP exchange model proposed by Faber et al. with the process Anonymity support, see Figure 5. As can be seen the Anonymity support process impacts all other processes. This is due to the fact that Anonymity support can be applied on any of the CP exchange model processes proposed by Faber et al. In addition to this enhancement, each of the processes/steps encompassed in the enhanced CP exchange model should also include all possible known alternatives that can be used to realize the process. Based on the information provided in Sections 2 and 3, we distinguish the following alternative solutions per each enhanced CP exchange model process.

4.1.1 Production
The possible alternative solutions that can be used to fulfill the Production category and are described in Sections 2 and 3 are the following:

- Abuse recording, see Section 2.1 and 3.6. Abuse recording and the used solutions can be found in Faber et al. [17]. An additional solution that can be classified in the Abuse recording process is the Webcam hacking described in [23, 26].

4.1.2 Hiding
The possible alternative solutions that can be used to fulfill the Hiding category and are described in Sections 2 and 3 are the following:

- Coding, see Section 2.1. Coding solutions can be found in Faber et al. [17]. The described features by Faber et al. are more elaborated in [33, 19, 32].
  - Untraceability: the disguise of the origin of the CP material. This mainly describes the deletion of metadata of a file.
  - Invisibility: the disguise of CP material without the use of external software. This mainly describes the altering of file extensions and file names.
  - Illegibility: the encryption of CP material.
  - Unrecognizability: the disguise of CP material with the use of external software. This mainly describes the stenography used to hide CP material inside other files and traffic.

4.1.3 Distribution
The possible alternative solutions that can be used to fulfill the Distribution category and are described in Sections 2 and 3 are the following:

- Acquire domain and hosting, see Section 2.1. Acquire domain and hosting are described by Faber et al. [17].
- Acquire customers, see Section 2.1, 2.2, 2.3 and 3.3. The acquiring of customers is described by Faber et al. [17], Wortley et al. [33], Van Wijk et al. [28] and is enhanced by the use of Anonymous remailers [29].
- Payment, see Sections 2.1, 2.3, 3.1, 3.2 and 3.5. Payment is originally described by Faber et al. [17] as financial transaction (money) and interchange of CP material, Van Wijk et al. In particular [28] elaborates and motivates the use of payment and interchange of CP material. Both processes are enhanced by the use of TOR [15], Freenet [13] and Anonymous credit cards [29].
- Distribution, see Sections 2.1, 2.2, 2.3, 2.4, 3.1, 3.2 and 3.3. Distribution is roughly described by Faber et al. [17], Wortley et al. [33] and Van Wijk et al. [28] and is more elaborated by Callanan et al. [12]. This process is enhanced by the use of TOR [15], Freenet [13] and Anonymous remailers [29].

4.1.4 Downloading
The possible alternative solutions that can be used to fulfill the Downloading category and are described in Sections 2 and 3 are the following:

- Downloading, see Sections 2.2, 2.3, 2.4, 3.1 and 3.2. Downloading is only briefly mentioned by Wortley et al. [33], Callanan et al. [12]. In particular, [12] elaborate this process in more detail. Characteristics of downloders are described by Van Wijk et al. [28]. The enhancements introduced by TOR [15] and Freenet [13] can also be applied to this process.

4.1.5 Storage
The possible alternative solutions that can be used to fulfill the Storage category and are described in Sections 2 and 3 are the following:

- Storage, see Sections 2.1, 2.3 and 3.4. Storage is briefly described by Faber et al. [17]. Van Wijk et al. [28] describes this process in more detail and introduces some aspects of physical storage. TrueCrypt [22] enhances this process.

4.1.6 Anonymity support
The possible alternative solutions that can be used to fulfill the ongoing Anonymity support and are described in Sections 2 and 3 are the following:

- Production
  - Webcam hacks, see Section 3.6. Webcam hacks [23, 26] provides anonymity for producers of CP material. Producers can groom and consolidate children into recording CP material using their own webcam if they are confronted with secretly earlier recorded material by the producer.
• Hiding
  – Hiding identity, see Section 2.1.
  
  Unrecognizability, illegibility, invisibility and untraceability of CP material provide additional anonymity for the producer of this CP material [17]. These techniques can be used to hide the identity of the producer before it gets distributed to a distributor.

• Distribution
  – Anonymous credit cards, see Section 3.5.
  Anonymous credit cards [29]: provides additional anonymity for distributors to register their domain and hosting. It also enhances the payment process.
  – Anonymous remailers, see Section 3.3.
  Anonymous remailers [29]: provides additional anonymity for distributors to acquire customers for their commercial CP website.
  – TOR, see Section 3.1.
  TOR [15]: provides additional anonymity for costumers of commercial CP websites. It furthermore enhances the anonymity of other CP related internet surfing.
  – Hidden services by TOR, see Section 3.1.
  TOR [15]: provides additional anonymity for distributors of CP material.
  – Freenet (Darknet mode), see Section 2.4 and 3.2.
  Freenet [13, 12]: provides additional anonymity for distributors of CP material.

• Downloading
  – TOR, see Section 3.1.
  TOR [15]: provides additional anonymity for downloaders / viewers of CP material.
  – Freenet [13, 12] (Darknet mode), see Section 2.4 and 3.2.
  Freenet [13, 12]: provides additional anonymity for downloaders of CP material.

• Storage
  – textitStorage, see Section 3.4.
  TrueCrypt [22]: provides additional anonymity for the storage of CP material.

Several processes in the proposed criminal CP exchange model can be modeled in combination with the Anonymity support process, see Figure 5.

4.2 Graphical representation
This section describes how the reader should interpret the graphical representation in Figure 5. The graphical representation of the model is roughly built as an activity diagram as proposed by the UML standard [16]. The process starts with the closed circle on the left going to the first category, which is Production. Each arrow represents the closure of one step and the beginning of a new one (the start and the end of the arrow respectively). After the first few processes, there is a branch / choice (drawn as a black rectangle) after which there are three different methods of distribution. The post-order distribution is not included in this research. After the Distribution, Downloading and Storage categories, the steps end in the closed circle with the open circle around it.

4.3 Verification
The verification of this newly proposed criminal CP exchange model is done by interviewing seven police detectives involved in the recent CP cases in the Netherlands. They belong to the Netherlands’ police agency (governmental police agency). The detectives that have been interviewed have different backgrounds in CP or IT studies.

In general the police detectives agree with the newly structured sequence of events in the criminal CP exchange process. They see it as a valuable addition to the earlier proposed exchange model by Faber et al. (Figure 1) and where different Distribution methods are split according to the results provided by Van Wijk et al. (Figure 3). The police detectives are not convinced that the Editing process should not be included in the Hiding category. They argue that the Editing process also involves the masking of the child abuser and therefore belongs to the Hiding category.

The results of the interview with the police detectives about the new proposed exchange model are analyzed and given below:

• Production
  Abuse recording: The use of the Abuse Recording step defined by Faber et al. [17] is found by the detectives to be modeled satisfactorily enough in order to describe the Production process. The enhancement described by the Webcam hacking [23, 26] has not been observed by the interviewed police detectives in practice (i.e. during their daily work) yet. Though, colleague detectives from foreign countries have observed child abusers chatting about this option, but it is not certain whether it has really happened and used in practice.

• Hiding
  Coding: The mentioned techniques deduced from Faber et al. [17] untraceability, invisibility, illegibility and unrecognizability are partly recognized by the police detectives. In particular, they have observed several of cases in practice where the encryption (illegibility) and deletion of metadata (untraceability) have been used. The use of external software (stenography in unrecognizability) though, is hardly observed in practice.

• Distribution
  – Acquire domain and hosting: these processes are observed by police detectives in practice, though, only in foreign countries. Up to now, the police have not seen any cases in which Dutch CP users have registered Internet based domains and hosting to build a commercial CP website. The information deduced from Faber et al. [17] is found as being accurate, since the detectives have observed this activity also in practice.

  – Acquire customers: as with the Acquire domain and hosting processes, police detectives were only aware of foreign cases in which the active acquiring of customers is observed. The use of Anonymous remailers as suggested by the enhancements though, has not yet been observed in practice.

  – Payment: as with the Acquire domain, hosting and customers processes, police detectives were
only aware of foreign cases in which the receiving of Payments were processed. Though, there are cases in which Dutch CP users have paid to watch CP material on commercial websites and where in all of these cases, credit card payments or different emoney payments were made. The enhancement proposed by the Anonymous credit cards have not been observed by the police detectives, in practice. The detectives do not expect to see this activity happening in the future in the Netherlands since buying such Credit Cards in the Netherlands is really hard.

Distribution: the distribution that is proposed by Faber et al. [17], Wortley et al. [33] and Van Wijk et al. [28] are found by the detectives to be outdated. The new distribution methods are far more anonymized (e.g., Freenet [13] and TOR hidden services [15]). Therefore the proposed enhancements are found to be very valuable. Usenet, Fora, FTP, e-mail, etc. are not anymore being observed by police detectives in their daily police activities.

- Downloading
  Downloading: the police detectives emphasized that the most of the downloading takes place anonymously since the distribution only prescribe downloading methods that are anonymous. Among them are browsing with the use of TOR [15] and downloading CP material with the use of Freenet [13]. The police detectives emphasized that the characteristics that are described by Van Wijk et al. [28] give a valuable insight into the group of CP users.

- Storage
  Storage: the police detectives expected an elaborated description on the categorization obsession of CP material downloadees. The obsession is roughly described by Van Wijk et al. [28] in the Downloading process, but it could also be stretched/placed to the Storage process, since it influences the way the storage of CP material is arranged. The enhancement of the Storage process with the use of TrueCrypt is sometimes observed in practice, but not often.

5. Conclusions and Future Work

This paper focused on how the currently used main criminal exchange models of child pornography can be adapted in order to describe (1) the current child pornography user behavior and (2) the new Internet based communication media and anonymization techniques used by child pornography offenders. Several research questions are derived and are answered by this paper.

Section 2 answers research question (1), by describing four different criminal CP exchange models [17, 33, 28, 12]. Faber et al. [17] is the most elaborated model.

Section 3 answers research question (2), by providing the technical enhancements on the CP criminal exchange models. In particular, six different enhancements to the existing CP exchange models were given, including The Onion Routing, Freenet, Anonymous remailers, TrueCrypt, Anonymous credit cards and Webcam hacks.

Section 4 answers research question (3) by proposing a new criminal CP exchange model that is verified by using interviews with seven police detectives of the Netherlands’ police agency that are concerned with the recent arrests of several child pornography offenders. The newly proposed CP exchange model has found its basis in the model proposed by Faber et al. [17] since this is the most elaborated one.

The enhancements made to the model by Faber et al. include (1) process enhancements and (2) technical enhancements. The process enhancements make it clearer that there is a distinction between three different distribution techniques: commercial websites, post-order and open / closed networks. The technical enhancements model is related to the Anonymity support that is omitted in the model proposed by Faber et al. [17] and other researches. By analyzing these enhancements, including the earlier proposed anonymization techniques, it could be de-
duced that Anonymity impacts all processes available in the criminal CP exchange model.

Future work includes three major research activities that could be undertaken. First of all, the list of enhancements proposed in Section 3 of this research is far from complete. These enhancements are selected by the mere creativity of the author and could be researched more thoroughly (possibly including police detectives). The verification of the proposed model should be performed more thoroughly. This could be done using case studies based on real police cases, or by interviewing a higher number of police detectives, e.g., from local police agencies or from other countries. Finally, the effectiveness of this new proposed model should be measured in practice.

6. REFERENCES