

Μαρία Αρετή

Γερμανού 57807

7ο Εξάμηνο 2022



ΔΗΜΟΚΡΙΤΕΙΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΡΑΚΗΣ DEMOCRITUS
UNIVERSITY OF THRACE

Όραση Υπολογιστών

Τεχνική Αναφορά - Εργασία 1η

Η τεχνική αναφορά περιλαμβάνει:

- I. Την θεωρητική ανάλυση της εργασίας.
- II. Την περιγραφή του κώδικα που παραδόθηκε.
- III. Την ανάλυση των αποτελεσμάτων.

I. Θεωρητική ανάλυση της εργασίας.

Σύμφωνα με την εκφώνηση της πρώτης εργασίας, θα πρέπει να αναλυθούν δομές εγγράφων που δίνονται σε αντίστοιχο φάκελο, να αναλυθούν οι υποπεριοχές τους και να τα αποτελέσματα να αποθηκευτούν εκ νέου με τις υποπεριοχές πλέον αναγνωρισμένες. Αναλυτικά θα παρουσιαστεί κάθε βήμα στην περιγραφή του κώδικα που θα γίνει παρακάτω και μαζί θα αναλυθούν και τα αποτελέσματα. Προς το παρόν ας παρουσιαστεί βηματικά η θεωρητική ανάλυση και μεθοδολογία που θα ακολουθηθεί παρακάτω.

// Εφαρμογή Φίλτρου Απόρριψης Θορύβου:

Αρχικά πρέπει να επιλέξουμε ένα φίλτρο απόθρυβοποίησης καθώς οι εικόνες που δίνονται έχουν θόρυβο τύπου "salt and pepper" ή αλλιώς "impulse noise". Ο συγκεκριμένος θόρυβος, χαρακτηρίζεται από την τοποθέτηση με τυχαίο τρόπο, μαύρων και λευκών εικονοστοιχείων μέσα στην εικόνα, δηλαδή τιμές 255 και 0 σε ένα grayscale κανάλι. Υπάρχουν διάφοροι τρόποι για να γίνει η απόθρυβοποίηση. Πριν παρουσιάσουμε τους τρόπους ας δείξουμε ένα παράδειγμα τέτοιου θορύβου.



Salt Noise Image

Pepper Noise Image

Both Salt and Pepper Noise Image

// Τρόποι Απόθρυβοποίησης:

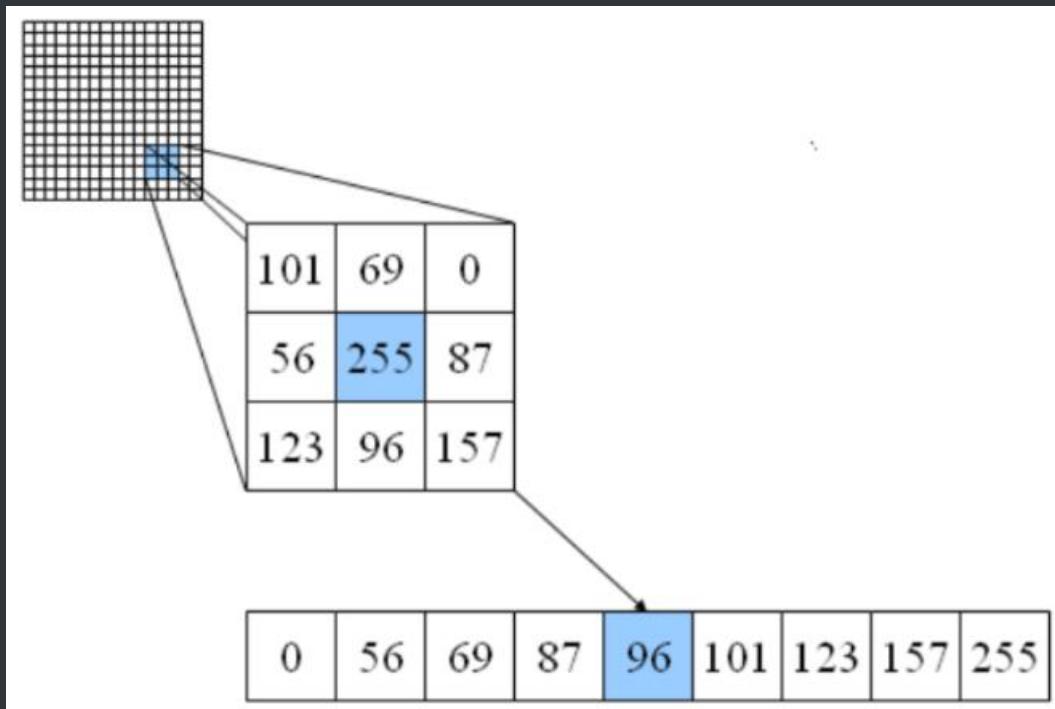
Υπάρχουν περισσότεροι τρόποι απόθρυβοποίησης από αυτούς που θα χρησιμοποιηθούν σε αυτή την εργασία εστιάζοντας κυρίως στα "Median Filters".

I. Θεωρητική ανάλυση της εργασίας.

Συγκεκριμένα μερικοί τρόποι:

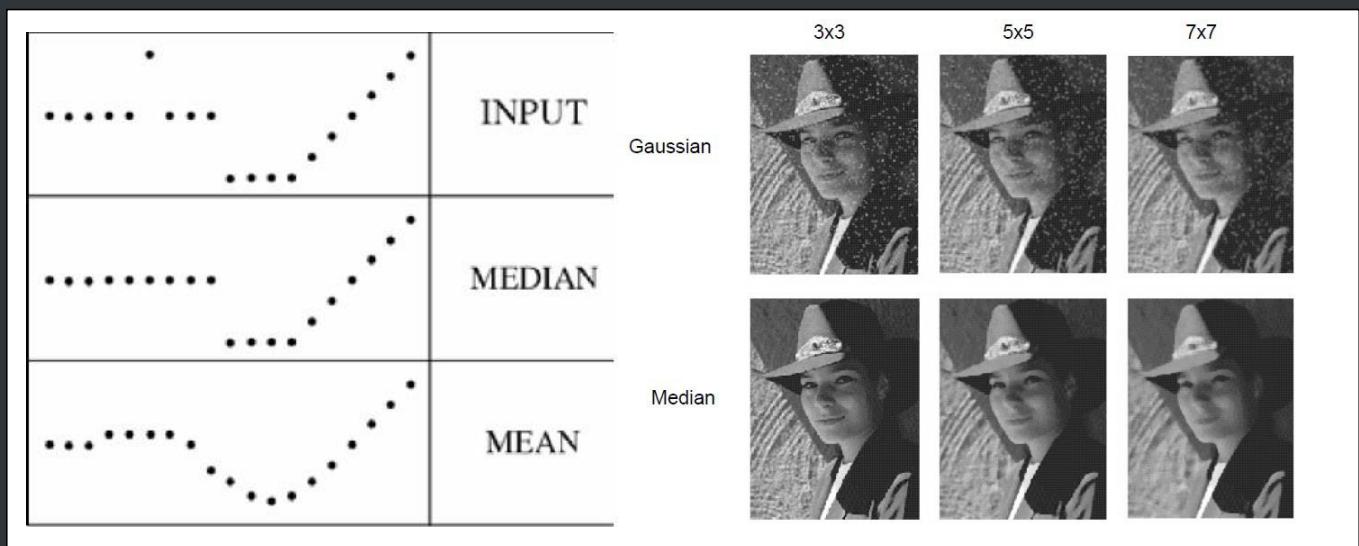
- Median Filtering.
- Gaussian Filtering.
- Mean Filtering.
- Opening.
- Closing.

Στην συγκεκριμένη περίπτωση θα γίνει χρήση ενός median filter, καθώς είναι απλή η υλοποίηση του, ακόμη και χωρίς την χρήση συναρτήσεων της βιβλιοθήκης "OpenCV". Συγκεκριμένα αυτό που κάνει ένα median filter είναι να αντικαθιστά την τιμή ενός pixel με την μεσαία τιμή των pixels ενός παραθύρου όπου κέντρο του είναι το pixel το οποίο θέλουμε να αντικαταστήσουμε. Ενδείκνυται σε αντίθεση με το "Mean Filtering" διότι το πρώτο είναι λιγότερο θολό από το δεύτερο και επιπλέον δέχεται τιμές που δεν δέχεται ένα απλό φίλτρο υπολογισμού μέσου όρου.



Στην υλοποίηση επίσης θα διασφαλιστεί πως το φίλτρο δεν θα βγαίνει εκτός των ορίων της εικόνας, έτσι επιλέχθηκε να γίνεται "padding" στην εικόνα ανάλογα με το μέγεθος του φίλτρου. Μόλις παραχθεί το αποτέλεσμα θα αφαιρείται και δεν θα εφαρμόζεται το φίλτρο στα όρια.

I. Θεωρητική ανάλυση της εργασίας.



// Υλοποίηση "Median Filter":

Αρχικά λοιπόν διαβάζουμε μία εικόνα και στην συνέχεια την μετατρέπουμε σε grayscale. Επειτα δημιουργούμε μια νέα εικόνα, η οποία είναι αντίγραφο της αρχικής με padding κατά 1. Δημιουργούμε δύο πίνακες στους οποίους τοποθετούμε τις τιμές των κεντρικών pixels και των γειτονικών pixels, που διαβάζονται στην επανάληψη, αντίστοιχα δημιουργώντας το παράθυρο για κάθε pixel. Στην συνέχεια ταξινομούμε τις τιμές και επιλέγουμε την μεσαία τιμή κάθε παραθύρου. Με αυτόν το τρόπο σαρώνουμε όλη την εικόνα. Τέλος αφαιρούμε το περίγραμμα που προσθέσαμε και η εικόνα επανέρχεται στις αρχικές της διαστάσεις. Παρατηρούμε ότι το αποτέλεσμα από την αποθορυβοποίηση και στις δυο περιπτώσεις είναι ικανοποιητικό. Πιο συγκεκριμένα όταν εφαρμόζουμε το median filter στην εικόνα με θόρυβο μπορούμε να δούμε πως όταν ο θόρυβος ήταν πάνω σε γράμματα τότε υπάρχει αλλοίωση σε αυτό ενώ όταν εφαρμόζουμε το φίλτρο στην αρχική εικόνα απλά αλλοιώνεται ελάχιστα η ποιότητα της εικόνας. Επιπλέον γίνεται σύγκριση και των αποτελεσμάτων της χρήσης του "Median Filtering" της "OpenCV" με την συνάρτηση που δημιουργήθηκε ώστε να ικανοποιεί τις λειτουργίες του "Median Filtering".

Σύγκριση αποθορυβοποιημένης εικόνας με την χρήση του φίλτρου και της "original" αποθορυβοποιημένης:

I. Θεωρητική ανάλυση της εργασίας.

implications of building viewer or consumer profiles through data mining, within the context of VPM and in light of the reaction it already has prompted [2]. Our intent is not to answer all of the questions here, but rather to outline the issues and to propose a framework within which both academics and practitioners can further explore the issue of privacy. Our analysis centers around three essential issues involving technology and privacy: stakeholder perceptions regarding the fairness of the process used by a company for collecting and distributing personal information, including the level of choice provided to the individual regarding whether and to what extent they will provide access to their personal characteristics; stakeholder perceptions regarding the fairness of the outcomes of those processes, including the cost-benefit trade-offs inherent in the exchange of personal information for some real or perceived gain; and stakeholder perceptions regarding the accuracy of inferred personal information—particularly the differential perceptions of consumers and advertisers regarding

TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial.

the impact of accurate versus inaccurate profiles. The analytic capability of VPM adds a layer of complexity to these issues by increasing the ability of a company to gather personal (viewing) information in an exceptionally unobtrusive manner, and then to use that information to infer individual demographic characteristics.

NEW THREATS TO PRIVACY THROUGH VIEWER PROFILING
The new threat to privacy begins with the basic technology of the Personal Video Recorder (PVR), which is able to directly monitor and report the viewing choices of individuals. To some extent, this is a reflection of the increased monitoring of individual behavior through a variety of data-gathering means, including point-of-sale devices, online ordering forms, and product registration requests. It also

includes less salient technologies such as spyware, which is conceptually similar to the PVR in its PC-based monitoring and reporting capabilities [10]. As we note later, the main difference between the PVR and spyware is that while PVR companies attempt to communicate their data collection and usage procedures in clearly worded privacy policies, spyware often skirts ethical constraints by installing itself on a user's PC with little or no advance warning.

The other major privacy issue in turn involves treatment of the information after it is collected. TiVo, a leading PVR manufacturer and service provider, is selling the viewing behaviors of its customers to Nielsen Media Research, which in turn will use that information to enhance its own collection and analysis of television viewing [6]. The type of information collected can be exceptionally detailed. TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial. Not surprisingly, this simple ability to collect viewing data, combined with the increasing number of PVRs in homes, has raised concerns from privacy advocates [1, 3].

The monitoring-profiling capabilities of the PVR have a direct impact on each of the stakeholders involved in the creation, distribution, and consumption of television advertising. In the domain of PVR-based targeted advertising, the direct stakeholders include television viewers, PVR providers, service providers (for example, cable and satellite companies), content providers (for example, broadcast and cable networks), and advertisers. The impact on these stakeholders can be explored, in turn, in the context of the three privacy issues raised earlier: procedures used to collect and distribute information, the perceived outcomes of those procedures, and the accuracy of inferred personal information. We discuss each of these issues, in part using TiVo as an example when appropriate, and then summarize the issues within a proposed framework for further investigation.

120 May 2006/Vol. 49, No. 5 COMMUNICATIONS OF THE ACM

My Median denoised image (not OpenCV function)

implications of building viewer or consumer profiles through data mining, within the context of VPM and in light of the reaction it already has prompted [2]. Our intent is not to answer all of the questions here, but rather to outline the issues and to propose a framework within which both academics and practitioners can further explore the issue of privacy. Our analysis centers around three essential issues involving technology and privacy: stakeholder perceptions regarding the fairness of the process used by a company for collecting and distributing personal information, including the level of choice provided to the individual regarding whether and to what extent they will provide access to their personal characteristics; stakeholder perceptions regarding the fairness of the outcomes of those processes, including the cost-benefit trade-offs inherent in the exchange of personal information for some real or perceived gain; and stakeholder perceptions regarding the accuracy of inferred personal information—particularly the differential perceptions of consumers and advertisers regarding

the impact of accurate versus inaccurate profiles, which is conceptually similar to the PVR in its PC-based monitoring and reporting capabilities [10]. As we note later, the main difference between the PVR and spyware is that while PVR companies attempt to communicate their data collection and usage procedures in clearly worded privacy policies, spyware often skirts ethical constraints by installing itself on a user's PC with little or no advance warning.

The other major privacy issue in turn involves treatment of the information after it is collected. TiVo, a leading PVR manufacturer and service provider, is selling the viewing behaviors of its customers to Nielsen Media Research, which in turn will use that information to enhance its own collection and analysis of television viewing [6]. The type of information collected can be exceptionally detailed. TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial. Not surprisingly, this simple ability to collect viewing data, combined with the increasing number of PVRs in homes, has raised concerns from privacy advocates [1, 3].

The monitoring-profiling capabilities of the PVR have a direct impact on each of the stakeholders involved in the creation, distribution, and consumption of television advertising. In the domain of PVR-based targeted advertising, the direct stakeholders include television viewers, PVR providers, service providers (for example, cable and satellite companies), content providers (for example, broadcast and cable networks), and advertisers. The impact on these stakeholders can be explored, in turn, in the context of the three privacy issues raised earlier: procedures used to collect and distribute information, the perceived outcomes of those procedures, and the accuracy of inferred personal information. We discuss each of these issues, in part using TiVo as an example when appropriate, and then summarize the issues within a proposed framework for further investigation.

TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial.

the impact of accurate versus inaccurate profiles. The analytic capability of VPM adds a layer of complexity to these issues by increasing the ability of a company to gather personal (viewing) information in an exceptionally unobtrusive manner, and then to use that information to infer individual demographic characteristics.

NEW THREATS TO PRIVACY THROUGH VIEWER PROFILING
The new threat to privacy begins with the basic technology of the Personal Video Recorder (PVR), which is able to directly monitor and report the viewing choices of individuals. To some extent, this is a reflection of the increased monitoring of individual behavior through a variety of data-gathering means, including point-of-sale devices, online ordering forms, and product registration requests. It also

includes less salient technologies such as spyware, which is conceptually similar to the PVR in its PC-based monitoring and reporting capabilities [10]. As we note later, the main difference between the PVR and spyware is that while PVR companies attempt to communicate their data collection and usage procedures in clearly worded privacy policies, spyware often skirts ethical constraints by installing itself on a user's PC with little or no advance warning.

The other major privacy issue in turn involves treatment of the information after it is collected. TiVo, a leading PVR manufacturer and service provider, is selling the viewing behaviors of its customers to Nielsen Media Research, which in turn will use that information to enhance its own collection and analysis of television viewing [6]. The type of information collected can be exceptionally detailed. TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial. Not surprisingly, this simple ability to collect viewing data, combined with the increasing number of PVRs in homes, has raised concerns from privacy advocates [1, 3].

TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial.

the impact of accurate versus inaccurate profiles. The analytic capability of VPM adds a layer of complexity to these issues by increasing the ability of a company to gather personal (viewing) information in an exceptionally unobtrusive manner, and then to use that information to infer individual demographic characteristics.

NEW THREATS TO PRIVACY THROUGH VIEWER PROFILING
The new threat to privacy begins with the basic technology of the Personal Video Recorder (PVR), which is able to directly monitor and report the viewing choices of individuals. To some extent, this is a reflection of the increased monitoring of individual behavior through a variety of data-gathering means, including point-of-sale devices, online ordering forms, and product registration requests. It also

includes less salient technologies such as spyware, which is conceptually similar to the PVR in its PC-based monitoring and reporting capabilities [10]. As we note later, the main difference between the PVR and spyware is that while PVR companies attempt to communicate their data collection and usage procedures in clearly worded privacy policies, spyware often skirts ethical constraints by installing itself on a user's PC with little or no advance warning.

The other major privacy issue in turn involves treatment of the information after it is collected. TiVo, a leading PVR manufacturer and service provider, is selling the viewing behaviors of its customers to Nielsen Media Research, which in turn will use that information to enhance its own collection and analysis of television viewing [6]. The type of information collected can be exceptionally detailed. TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial. Not surprisingly, this simple ability to collect viewing data, combined with the increasing number of PVRs in homes, has raised concerns from privacy advocates [1, 3].

TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial.

the impact of accurate versus inaccurate profiles. The analytic capability of VPM adds a layer of complexity to these issues by increasing the ability of a company to gather personal (viewing) information in an exceptionally unobtrusive manner, and then to use that information to infer individual demographic characteristics.

120 May 2006/Vol. 49, No. 5 COMMUNICATIONS OF THE ACM

Original denoised image

implications of building viewer or consumer profiles through data mining, within the context of VPM and in light of the reaction it already has prompted [2]. Our intent is not to answer all of the questions here, but rather to outline the issues and to propose a framework within which both academics and practitioners can further explore the issue of privacy. Our analysis centers around three essential issues involving technology and privacy: stakeholder perceptions regarding the fairness of the process used by a company for collecting and distributing personal information, including the level of choice provided to the individual regarding whether and to what extent they will provide access to their personal characteristics; stakeholder perceptions regarding the fairness of the outcomes of those processes, including the cost-benefit trade-offs inherent in the exchange of personal information for some real or perceived gain; and stakeholder perceptions regarding the accuracy of inferred personal information—particularly the differential perceptions of consumers and advertisers regarding

the impact of accurate versus inaccurate profiles, which is conceptually similar to the PVR in its PC-based monitoring and reporting capabilities [10]. As we note later, the main difference between the PVR and spyware is that while PVR companies attempt to communicate their data collection and usage procedures in clearly worded privacy policies, spyware often skirts ethical constraints by installing itself on a user's PC with little or no advance warning.

The other major privacy issue in turn involves treatment of the information after it is collected. TiVo, a leading PVR manufacturer and service provider, is selling the viewing behaviors of its customers to Nielsen Media Research, which in turn will use that information to enhance its own collection and analysis of television viewing [6]. The type of information collected can be exceptionally detailed. TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial. Not surprisingly, this simple ability to collect viewing data, combined with the increasing number of PVRs in homes, has raised concerns from privacy advocates [1, 3].

TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial.

the impact of accurate versus inaccurate profiles. The analytic capability of VPM adds a layer of complexity to these issues by increasing the ability of a company to gather personal (viewing) information in an exceptionally unobtrusive manner, and then to use that information to infer individual demographic characteristics.

NEW THREATS TO PRIVACY THROUGH VIEWER PROFILING
The new threat to privacy begins with the basic technology of the Personal Video Recorder (PVR), which is able to directly monitor and report the viewing choices of individuals. To some extent, this is a reflection of the increased monitoring of individual behavior through a variety of data-gathering means, including point-of-sale devices, online ordering forms, and product registration requests. It also

includes less salient technologies such as spyware, which is conceptually similar to the PVR in its PC-based monitoring and reporting capabilities [10]. As we note later, the main difference between the PVR and spyware is that while PVR companies attempt to communicate their data collection and usage procedures in clearly worded privacy policies, spyware often skirts ethical constraints by installing itself on a user's PC with little or no advance warning.

The other major privacy issue in turn involves treatment of the information after it is collected. TiVo, a leading PVR manufacturer and service provider, is selling the viewing behaviors of its customers to Nielsen Media Research, which in turn will use that information to enhance its own collection and analysis of television viewing [6]. The type of information collected can be exceptionally detailed. TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial. Not surprisingly, this simple ability to collect viewing data, combined with the increasing number of PVRs in homes, has raised concerns from privacy advocates [1, 3].

TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial.

the impact of accurate versus inaccurate profiles. The analytic capability of VPM adds a layer of complexity to these issues by increasing the ability of a company to gather personal (viewing) information in an exceptionally unobtrusive manner, and then to use that information to infer individual demographic characteristics.

NEW THREATS TO PRIVACY THROUGH VIEWER PROFILING
The new threat to privacy begins with the basic technology of the Personal Video Recorder (PVR), which is able to directly monitor and report the viewing choices of individuals. To some extent, this is a reflection of the increased monitoring of individual behavior through a variety of data-gathering means, including point-of-sale devices, online ordering forms, and product registration requests. It also

120 May 2006/Vol. 49, No. 5 COMMUNICATIONS OF THE ACM

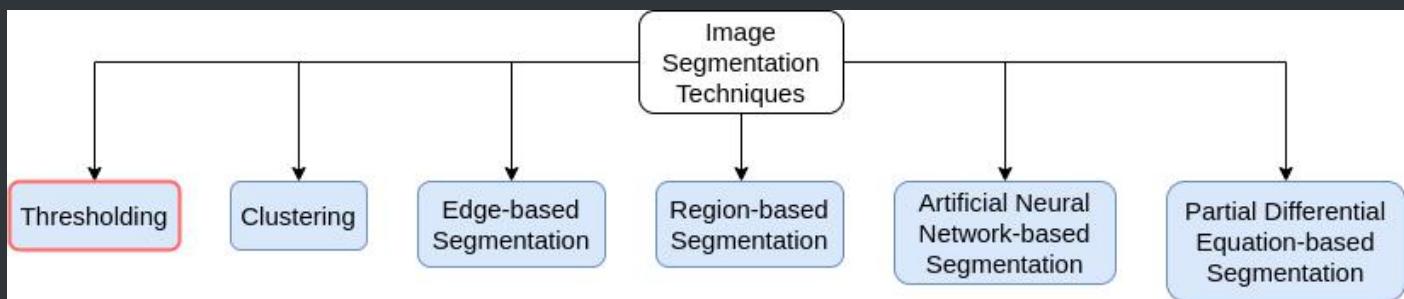
Median denoised image

My Median denoised image

I. Θεωρητική ανάλυση της εργασίας.

// Ανίχνευση όλων των υποπεριοχών και μετρήσεις: Δημιουργία Δυαδικής Εικόνας

Για να μπορέσουμε να εντοπίσουμε και έπειτα να χωρίσουμε την εικόνα σε υποπεριοχές, πρέπει να γίνουν κάποιες μορφολογικές πράξεις στις οποίες θα αναφερθούμε στην συνέχεια. Για να είναι δυνατό να κάνουμε αυτές τις πράξεις πρέπει να μετατρέψουμε την εικόνα σε δυαδική (Binary Image). Πριν την μετατροπή μιας grayscale εικόνας σε binary επιλέγεται μια τιμή του γκρι, "threshold", όπου αν κάποιο pixel έχει τιμή μεγαλύτερη από αυτή θα γίνει τελείως λευκό (255) ενώ αν έχει μικρότερη από αυτή θα γίνει τελείως μαύρο (0). Αυτή η τιμή μπορεί να βρεθεί με δύο τρόπους, ένας τρόπος είναι κάθε φορά με trial and error να βρίσκεται μια καλή τιμή. Άλλος τρόπος που θα χρησιμοποιηθεί και στην εργασία είναι η χρήση του αλγόριθμου "Otsu's Thresholding", η οποία επιλέγει αυτόματα την καταλληλότερη τιμή για threshold για κάθε περίπτωση. Συγκεκριμένα ο αλγόριθμος επεξεργάζεται την εικόνα της εισόδου, αποκτά το "histogram" της εικόνας, την κατανομή των pixels και υπολογίζει την ζητούμενη τιμή της μεταβλητής αυτόματα. Στην ανάλυση του κώδικα θα φανεί η τιμή του threshold που επιλέχθηκε και το αποτέλεσμα που εκτυπώνουμε στην οθόνη. Η μέθοδος που αναλύθηκε είναι μία από τις τεχνικές "Image Segmentation". Σε επόμενες εργασίες θα χρησιμοποιηθούν και άλλες τεχνικές όπως αναφέρονται στην παρακάτω εικόνα.



// Επιλογή συνδυασμού μορφολογικών μετασχηματισμών:

Σε αυτό το σημείο θα επιλεχθούν οι μετασχηματισμοί για τον χωρισμό των περιοχών και έπειτα για την καταμέτρηση των λέξεων. Υπάρχουν διάφοροι συνδυασμοί μετασχηματισμών οι οποίοι μπορούν να μας οδηγήσουν στο επιθυμητό αποτέλεσμα. Μερικοί μετασχηματισμοί που θα χρησιμοποιηθούν είναι το dilation και το erosion. Υπάρχουν και οι opening και closing αλλά είναι συνδυασμός των dilation και erosion με διαφορετική σειρά. Opening είναι η ακολουθία

I. Θεωρητική ανάλυση της εργασίας.

που δεν μας ενδιαφέρει. Σε αυτήν την περίπτωση αυξάνεται ο αριθμός περιοχών που αγνοήθηκαν και προχωράμε στην επόμενη επανάληψη χωρίς να σχεδιάσουμε και να κάνουμε μετρήσεις. Σε περίπτωση λοιπόν που δεν ως και ή μεγαλύτερα του 15, δηλαδή για την περίπτωση που έχουμε μια υποπεριοχή, έχοντας τις συντεταγμένες για το bounding box μέσω της συνάρτησης rectangle σχεδιάζουμε στην αρχική μας εικόνα ένα περιβάλλον κουτί και στην συνέχεια γράφουμε έναν αριθμό μέσω της της συνάρτησης "Put Text". Τώρα για τον υπολογισμό του εμβαδού του bounding box χρειαζόμαστε απλά το πλάτος και το ύψος του. Ο υπολογισμός γίνεται ως εξής. Το εμβαδόν είναι μήκος επί πλάτος. Τα υπόλοιπα στοιχεία που χρειάζεται να υπολογιστούν αναλύθηκαν θεωρητικά και θα αναφερθούν στην ανάλυση κώδικα.

// Περιγραφή Κώδικα: Φόρτωση εικόνων σε Path και ανάγνωσή τους με την OpenCV σε ασπρόμαυρη μορφή.

```
# Re-assigning the files:  
filenames_org_1 = 'images/1_original.png'  
filenames_org_2 = 'images/2_original.png'  
filenames_org_3 = 'images/3_original.png'  
filenames_org_4 = 'images/4_original.png'  
filenames_org_5 = 'images/5_original.png'  
  
filenames_ns_1 = 'images/1_noise.png'  
filenames_ns_2 = 'images/2_noise.png'  
filenames_ns_3 = 'images/3_noise.png'  
filenames_ns_4 = 'images/4_noise.png'  
filenames_ns_5 = 'images/5_noise.png'  
  
img_o_1 = cv2.imread(filenames_org_1, cv2.IMREAD_GRAYSCALE)  
img_o_2 = cv2.imread(filenames_org_2, cv2.IMREAD_GRAYSCALE)  
img_o_3 = cv2.imread(filenames_org_3, cv2.IMREAD_GRAYSCALE)  
img_o_4 = cv2.imread(filenames_org_4, cv2.IMREAD_GRAYSCALE)  
img_o_5 = cv2.imread(filenames_org_5, cv2.IMREAD_GRAYSCALE)  
img_n_1 = cv2.imread(filenames_ns_1, cv2.IMREAD_GRAYSCALE)  
img_n_2 = cv2.imread(filenames_ns_2, cv2.IMREAD_GRAYSCALE)  
img_n_3 = cv2.imread(filenames_ns_3, cv2.IMREAD_GRAYSCALE)  
img_n_4 = cv2.imread(filenames_ns_4, cv2.IMREAD_GRAYSCALE)  
img_n_5 = cv2.imread(filenames_ns_5, cv2.IMREAD_GRAYSCALE)
```

// Περιγραφή Κώδικα: Χρήση της συνάρτησης "Median Filter" που δίνεται από την OpenCV και σύγκριση με το αποτέλεσμα της δημιουργημένης συνάρτησης που υπάρχει στο πρόγραμμα.

```
# using filter mean or median for de-noising grayscale images with opencv:  
median = cv2.medianBlur(img_n_1, 3)  
# cv2.namedWindow('median with open cv', cv2.WINDOW_NORMAL)  
# cv2.imshow('median with open cv', median)  
# cv2.waitKey(0)  
cv2.imwrite('org_median_denoised.png', median)
```

I. Θεωρητική ανάλυση της εργασίας.

Τα αποτελέσματα αυτά προβάλλονται παραπάνω δίπλα το ένα στο άλλο. Προς το παρόν θα περιγραφεί η διαδικασία της δημιουργημένης συνάρτησης. Αρχικά φτιάχνουμε ένα αντίγραφο της εικόνας που παίρνουμε ως όρισμα και μετά αποθηκεύουμε τις διαστάσεις της ως προς τον αριθμό των σειρών και των στηλών. Επειτα ταξινομούμε τις κεντρικές και γειτονικές τιμές που αποθηκεύονται προσωρινά ενός παραθύρου 3×3 και κατά αυτόν το τρόπο σαρώνουμε όλη την εικόνα.

```
# using filter mean or median for de-noising grayscale images without opencv:  
# firstly we use a function that forms a border around an image and applies the respective padding.  
# Then we define our window size and its half.  
# Constant value border: Applies a padding of a constant value for the whole border and its color  
is chosen randomly.  
def median_filter(img_noise):  
    # Check if image is loaded fine  
    # if img_noise is None:  
    #     print('Error opening image!')  
    #     return -1  
  
    # Creating a copy of image:  
    img_noise_2 = np.copy(img_noise)  
  
    rows = img_noise.shape[0]  
    cols = img_noise.shape[1]  
  
    for k in range(rows - 2):  
        for j in range(cols - 2):  
            temp = [img_noise[k][j], img_noise[k][j + 1], img_noise[k][j + 2], img_noise[k + 1][j],  
                    img_noise[k + 1][j + 1], img_noise[k + 1][j + 2],  
                    img_noise[k + 2][j], img_noise[k + 2][j + 1], img_noise[k + 2][j + 2]]  
            temp.sort()  
            img_noise_2[k + 1][j + 1] = temp[4]  
    return img_noise_2
```

Προχωρώντας στην δημιουργία της δυαδικής εικόνας, βρίσκεται αυτόματα η "flag" τιμή του αλγορίθμου και εκτυπώνεται στην οθόνη.

```
# Taking the resulting gray image from the de-noising above and transforming it to binary image.  
# We use Otsu's Binarization that chooses a value and determines it automatically:  
flag_otsu = cv2.THRESH_BINARY_INV + cv2.THRESH_OTSU  
  
thres1, th1 = cv2.threshold(median, 0, 255, flag_otsu)  
thres2, th2 = cv2.threshold(img_o_1, 0, 255, flag_otsu)  
  
# Also i save the resulted images and view the threshold binary image with and without noise  
cv2.imwrite('org_bin_otsu.png', th1)  
cv2.imwrite('ns_bin_otsu.png', th2)  
avg_thres = (thres1 + thres2) // 2  
print("Automatically chosen average value from Otsu's Binarization: ", avg_thres)
```

Automatically chosen average value from Otsu's Binarization: 174.0

II. Περιγραφή του κώδικα.

Προβάλουμε τα αποτελέσματα στις δύο εικόνες με θόρυβο και χωρίς αν εφαρμοστεί η μεθοδολογία δημιουργίας δυαδικής εικόνας. Παρατηρούμε ότι το binary αποτέλεσμα της original εικόνας είναι λίγο καλύτερο από αυτής με τον θόρυβο καθώς κατά την αποθορυβοποίηση της τελευταίας υπήρχε μερική αλλοίωση σε κάποια γράμματα.

implications of building viewer or consumer profiles through data mining, within the context of VPM and in light of the reaction it already has prompted [2]. Our intent is not to answer all of the questions here, but rather to outline the issues and to propose a framework within which both academics and practitioners can further explore the issue of privacy. Our analysis centers around three essential issues involving technology and privacy: stakeholder perceptions regarding the fairness of the process used by a company for collecting and distributing personal information, including the level of choice provided to the individual regarding whether and to what extent they will provide access to their personal characteristics; stakeholder perceptions regarding the fairness of the outcomes of those processes, including the cost-benefit trade-offs inherent in the exchange of personal information for some real or perceived gain; and stakeholder perceptions regarding the *accuracy of inferred personal information*—particularly the differential perceptions of consumers and advertisers regarding

includes less salient technologies such as spyware, which is conceptually similar to the PVR in its PC-based monitoring and reporting capabilities [10]. As we note later, the main difference between the PVR and spyware is that while PVR companies attempt to communicate their data collection and usage procedures in clearly worded privacy policies, spyware often skirts ethical constraints by installing itself on a user's PC with little or no advance warning.

The other major privacy issue in turn involves treatment of the information after it is collected. TiVo, a leading PVR manufacturer and service provider, is selling the viewing behaviors of its customers to Nielsen Media Research, which in turn will use that information to enhance its own collection and analysis of television viewing [6]. The type of information collected can be exceptionally detailed. TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial. Not surprisingly, this simple ability to collect viewing data, combined with the increasing number of PVRs in homes, has raised concerns from privacy advocates [1, 3].

The monitoring-profiling capabilities of the PVR have a direct impact on each of the stakeholders involved in the creation, distribution, and consumption of television advertising. In the domain of PVR-based targeted advertising, the direct stakeholders include television viewers, PVR providers, service providers (for example, cable and satellite companies), content providers (for example, broadcast and cable networks), and advertisers. The impact on these stakeholders can be explored, in turn, in the context of the three privacy issues raised earlier: procedures used to collect and distribute information, the perceived outcomes of those procedures, and the accuracy of inferred personal information. We discuss each of these issues, in part using TiVo as an example when appropriate, and then summarize the issues within a proposed framework for further investigation.

TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial.

the impact of accurate versus inaccurate profiles. The analytic capability of VPM adds a layer of complexity to these issues by increasing the ability of a company to gather personal (viewing) information in an exceptionally unobtrusive manner, and then to use that information to infer individual demographic characteristics.

NEW THREATS TO PRIVACY THROUGH VIEWER PROFILING
The new threat to privacy begins with the basic technology of the Personal Video Recorder (PVR), which is able to directly monitor and report the viewing choices of individuals. To some extent, this is a reflection of the increased monitoring of individual behavior through a variety of data-gathering means, including point-of-sale devices, online ordering forms, and product registration requests. It also

includes less salient technologies such as spyware, which is conceptually similar to the PVR in its PC-based monitoring and reporting capabilities [10]. As we note later, the main difference between the PVR and spyware is that while PVR companies attempt to communicate their data collection and usage procedures in clearly worded privacy policies, spyware often skirts ethical constraints by installing itself on a user's PC with little or no advance warning.

TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial.

Filtered Binary with Otsu's method: noise vs original

Σε αυτό το βήμα επιλέγονται οι μετασχηματισμοί που θα χρησιμοποιήσω αρχικά για τον εντοπισμό των περιοχών και στην συνέχεια για την καταμέτρηση των λέξεων. Για αρχή δημιουργώ τα "structural elements" που θα χρησιμοποιηθούν τα οποία μπορεί να έχουν διαφορετικά σχήματα και μεγέθη, εφαρμόζονται σε όλη την εικόνα και για κάθε pixel δίνεται τιμή ανάλογα με τον μετασχηματισμό που χρησιμοποιώ. Ο κώδικας για τον χωρισμό και εντοπισμό περιοχών βρίσκεται παρακάτω μαζί με τον αντίστοιχο κώδικα για τον χωρισμό λέξεων. Συγκεκριμένα

II. Περιγραφή του κώδικα.

εφαρμόζουμε “dilation and closing” στις εικόνες ώστε να ενωθούν οι λέξεις και έπειτα να ενωθούν τα κενά στα γράμματα στην κάθετη διεύθυνση. Τα αποτελέσματα φαίνονται παρακάτω στην εικόνα με θόρυβο μόνο καθώς δεν παρουσιάζονται μεγάλες διαφορές από την original.

```
# At this point its time to choose transforms to count words and divide areas of images. A combination of open and
# close transforms is used to connect the areas and words. Dilate and erosion consist the previous transformations.
# Structuring elements are being created to connect the areas by dilation, but this action will change the sizes of
# the areas and results will be wrong. So firstly words are being connected with each other. Also the closing next is
# used to fill vertically gaps of letters.

sqr_1 = np.ones((3, 3), np.uint8)
sqr_2 = np.ones((5, 5), np.uint8)
rect_1 = np.ones((1, 4), np.uint8)

# For text area dilation and closing:
temp2 = cv2.morphologyEx(th1, cv2.MORPH_DILATE, sqr_1, iterations=1)
texts_bound = cv2.morphologyEx(temp2, cv2.MORPH_CLOSE, sqr_2, iterations=8)
# For text area dilation and closing:
temp2 = cv2.morphologyEx(th1, cv2.MORPH_DILATE, sqr_1, iterations=1)
texts_bound = cv2.morphologyEx(temp2, cv2.MORPH_CLOSE, sqr_2, iterations=8)

# cv2.namedWindow("text_division", cv2.WINDOW_NORMAL)
# cv2.imshow("text_division", texts_bound)
# cv2.waitKey(0)
# For words dilation and closing:
temp = cv2.morphologyEx(th1, cv2.MORPH_DILATE, rect_1, iterations=3)
words_bound = cv2.morphologyEx(temp, cv2.MORPH_CLOSE, rect_1, iterations=1)

# cv2.namedWindow("word_division", cv2.WINDOW_NORMAL)
# cv2.imshow("word_division", words_bound)
# cv2.waitKey(0)

cv2.imwrite('text_division.png', texts_bound)
cv2.imwrite('word_division.png', words_bound)

# The connected components have been formed and the function is used to return the number of the components found.
num, val_pix = cv2.connectedComponents(texts_bound)

# The bounding boxes and measures to be done will be performed according to the number of components found.
To design
# the bounding boxes a function is used that stores the coordinates of the box. Through an array of zeros we create a
# mask which later will be helpful to calculate the dimensions of bounding box. An integral image is created in which
# every pixel is sum of its neighbors to the upper left. Also every pixel of looped area is set to 255. Height and
# width is checked with a limit - value, before we move on to the next loop because areas often are consisted by
# higher values than the limit we chose. This check is happening so trash - information will not be considered
# countable region
```

II. Περιγραφή του κώδικα.

Τα αποτελέσματα είναι ικανοποιητικά και στις δύο περιπτώσεις καθώς στην



text_division.png

word_division.png

πρώτη κάθε υποεριοχή έχει σχηματιστεί ένα συνδεδεμένο στοιχείο ενώ στην δεύτερη περίπτωση σχεδόν κάθε λέξη αποτελεί συνδεδεμένο στοιχείο. Στην συνέχεια πάμε σε κάθε περιοχή και σχεδιάζεται ένα περιβάλλον κουτί. Έπειτα δίνεται ένας μοναδικός αύξων αριθμός. Αρχικά, χρησιμοποιήθηκε η συνάρτηση "Connected Components" στην εικόνα η οποία επιστρέφει έναν αριθμό που δηλώνει πόσα διαφορετικά "Connected Components" βρέθηκαν και ένα πίνακα όπου η τιμή των pixel κάθε "Connected Components" έχει ένα συγκεκριμένο αριθμό. Η αριθμηση ξεκινάει από το 0 που λαμβάνεται ως τιμή από το background. Κατά την επανάληψη ελέγχεται αν κάθε pixel είναι λευκό και με τις διαστάσεις που δίνονται, σχεδιάζεται ένα ορθογώνιο. Για να σχεδιαστεί ένα bounding box χρειαζόμαστε τουλάχιστον τις συντεταγμένες της επάνω αριστερά γωνίας και τις κάτω δεξιά. Την πληροφορία αυτήν για κάθε περιοχή μπορούμε να την λάβουμε μέσω της συνάρτησης "Bounding Rect" η οποία επιστρέφει ως x, y τις συντεταγμένες της

αποφάσισης building blocks for consumer profiles through data mining, in the context of VPM and in light of the issues it already has proposed [2]. Our intent is not to answer all of the questions here, for rather to outline the issues and to propose a framework within which both academics and practitioners can further explore the issue of privacy. Our analysis covers around three essential issues involving technology and privacy: stakeholder perceptions regarding the fairness of the powers used by a company for collecting and distributing personal information, including the level of choice given to the individual regarding whether and to what extent they may grant access to their personal characteristics; stakeholder perceptions regarding the fairness of the outcomes of these processes, including the cost benefit trade-offs inherent in the exchange of personal information for some end or perceived gain; and stakeholder perceptions regarding the accuracy of inferred personal information, particularly the differential perceptions of consumers and audiences regarding

includes less efficient technologies such as spycam, which is conceptually similar to the PVR in its PC-based monitoring and reporting capabilities [10]. As we note later, the main difference between the PVR and spycam is that while PVR companies attempt to communicate their data collection and usage policies in clearly worded policy policies, spycam often skirts ethical concerns by installing itself on a user's PC with little or no advance warning.

The other major privacy issue in more advanced measurement of the information after it is collected, TiVo, a leading PVR manufacturer and service provider, is selling the viewing behaviors of its customers to Nielsen Media Research, which in turn will use that information to enhance its own collection and analysis of television viewing [11]. The type of information collected can be conveniently described. TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial.

TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial.

the impact of accurate versus inaccurate profiles. The analytic capability of VPM adds a layer of complexity to these issues by increasing the ability of a company to gather personal (viewing) information in an extremely indiscriminate manner, and then to use that information to infer additional demographic characteristics.

New Threats to Privacy through Viewer Profiling: The new threat to privacy begins with the basic technology of the Personal Video Recorder (PVR), which is able to directly collect and report the viewing choices of individuals. To some extent, this is a reflection of the increased monitoring of individual behavior through a variety of data-gathering means, including power of sale devices, online ordering forms, and product registration requests. It also

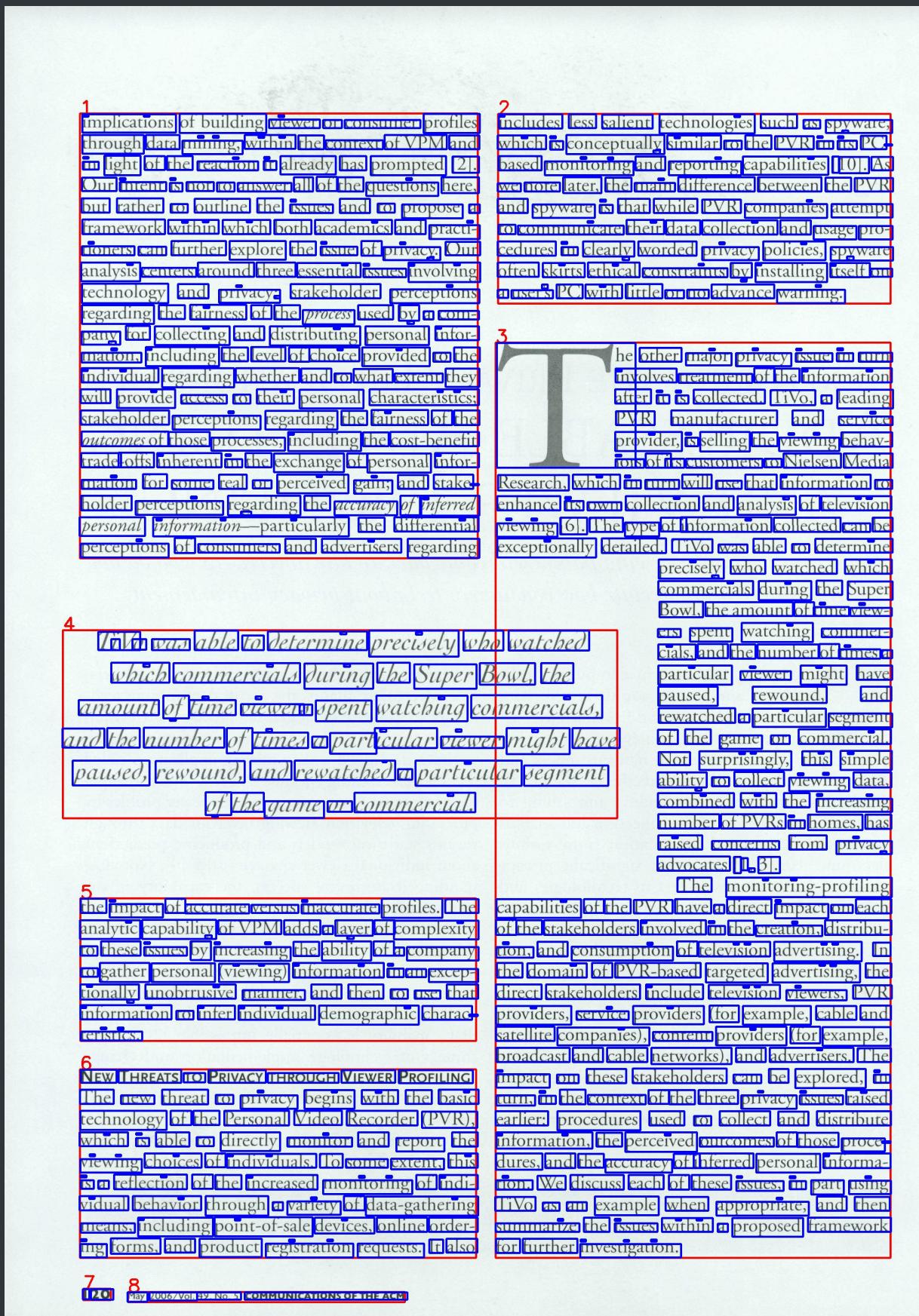
impacts the capabilities of the PVR have a direct impact on each of the stakeholders involved in the creation, distribution, and consumption of television advertising. In the domain of PVR-based targeted advertising, the direct stakeholders include television viewers, PVR providers, service providers (for example, cable and satellite companies), content providers (for example, broadcast and cable networks), and advertisers. The impact on these stakeholders can be explored, in the context of the three policy issues raised earlier: procedures used to collect and distribute information, the perceived outcomes of those procedures, and the accuracy of inferred personal information. We discuss each of these issues, in particular, TiVo as an example when appropriate, and then summarize the issues within a proposed framework for further investigation.

II. Περιγραφή του κώδικα.

// Υπολογισμός εμβαδού: Το εμβαδόν υπολογίζεται από το γινόμενο των διαστάσεων του κουτιού όπως φαίνεται και στον παραπάνω κώδικα.

1 implications of building viewer or consumer profiles through data mining, within the context of VPM and in light of the reaction it already has prompted [2]. Our intent is not to answer all of the questions here, but rather to outline the issues and to propose a framework within which both academics and practitioners can further explore the issue of privacy. Our analysis centers around three essential issues involving technology and privacy: stakeholder perceptions regarding the fairness of the <i>process</i> used by a company for collecting and distributing personal information, including the level of choice provided to the individual regarding whether and to what extent they will provide access to their personal characteristics; stakeholder perceptions regarding the fairness of the <i>outcomes</i> of those processes, including the cost-benefit trade-offs inherent in the exchange of personal information for some real or perceived gain; and stakeholder perceptions regarding the <i>accuracy of inferred personal information</i> —particularly the differential perceptions of consumers and advertisers regarding	2 includes less salient technologies such as spyware, which is conceptually similar to the PVR in its PC-based monitoring and reporting capabilities [10]. As we note later, the main difference between the PVR and spyware is that while PVR companies attempt to communicate their data collection and usage procedures in clearly worded privacy policies, spyware often skirts ethical constraints by installing itself on a user's PC with little or no advance warning.
4 <i>TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial.</i>	3 <p>The other major privacy issue in turn involves treatment of the information after it is collected. TiVo, a leading PVR manufacturer and service provider, is selling the viewing behaviors of its customers to Nielsen Media Research, which in turn will use that information to enhance its own collection and analysis of television viewing [6]. The type of information collected can be exceptionally detailed. TiVo was able to determine precisely who watched which commercials during the Super Bowl, the amount of time viewers spent watching commercials, and the number of times a particular viewer might have paused, rewound, and rewatched a particular segment of the game or commercial. Not surprisingly, this simple ability to collect viewing data, combined with the increasing number of PVRs in homes, has raised concerns from privacy advocates [1, 3].</p>
5 the impact of accurate versus inaccurate profiles. The analytic capability of VPM adds a layer of complexity to these issues by increasing the ability of a company to gather personal (viewing) information in an exceptionally unobtrusive manner, and then to use that information to infer individual demographic characteristics.	The monitoring-profiling capabilities of the PVR have a direct impact on each of the stakeholders involved in the creation, distribution, and consumption of television advertising. In the domain of PVR-based targeted advertising, the direct stakeholders include television viewers, PVR providers, service providers (for example, cable and satellite companies), content providers (for example, broadcast and cable networks), and advertisers. The impact on these stakeholders can be explored, in turn, in the context of the three privacy issues raised earlier: procedures used to collect and distribute information, the perceived outcomes of those procedures, and the accuracy of inferred personal information. We discuss each of these issues, in part using TiVo as an example when appropriate, and then summarize the issues within a proposed framework for further investigation.
6 NEW THREATS TO PRIVACY THROUGH VIEWER PROFILING The new threat to privacy begins with the basic technology of the Personal Video Recorder (PVR), which is able to directly monitor and report the viewing choices of individuals. To some extent, this is a reflection of the increased monitoring of individual behavior through a variety of data-gathering means, including point-of-sale devices, online ordering forms, and product registration requests. It also	7 8 May 2006/Vol. 49, No. 5 COMMUNICATIONS OF THE ACM

II. Περιγραφή του κώδικα.



bounding_box_colored_words.png

II. Περιγραφή του κώδικα.

// Υπολογισμός περιοχής κειμένου: Με παρόμοια επανάληψη εντοπίζουμε, χρησιμοποιώντας ένα παράθυρο αναζήτησης με διαστάσεις που ερευνούν από το ένα άκρο περιοχής στο άλλο, τα λευκά σημεία και αυξάνουμε τον μετρητή μας κατά ένα.

```
# Calculating text area:
text_area_box = th1[y:y + h, x:x + w]
text_area = 0
for y_i in range(1, text_area_box.shape[0]):
    for x_i in range(1, text_area_box.shape[1]):
        if text_area_box[y_i][x_i] == 255:
            text_area += 1

print("Text Area: ", text_area)
```

// Υπολογισμός μέσης τιμής διαβάθμισης του γκρι: Πρακτικά ο υπολογισμός που ζητείται είναι το άθροισμα των τιμών των pixel σε κάθε υποπεριοχή προς τον αριθμό των pixel του εμβαδού. Εδώ λοιπόν θα χρησιμοποιηθεί το Integral Image της grayscale αποθορυβοποιημένης εικόνας το οποίο μπορεί να υπολογίσει το άθροισμα των τιμών των pixel σε σταθερό χρόνο.

```
# Calculating Mean gray-level value in bounding box:
A = img_integral[y][x]
D = img_integral[y + h][x + w]
B = img_integral[y][x + w]
C = img_integral[y + h][x]
mglv = (A + D - B - C) / (w * h)
print("Mean Gray Value of bounding box: ", mglv)
```

Solution is found using:

$$A + D - B - C$$

