ΣΤΡΑΤΙΩΤΙΚΗ ΣΧΟΛΗ
ΕΥΕΛΠΙΔΩΝ
ΤΜΗΜΑ ΣΤΡΑΤΙΩΤΙΚΩΝ
ΕΠΙΣΤΗΜΩΝ

ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΠΑΡΑΓΩΓΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

Διιδρυματικό Διατμηματικό Πρόγραμμα
Μεταπτυχιακών Σπουδών
Σχεδίαση και Επεξεργασία Συστημάτων

Η Κυβερνοεπίθεση στην Επικοινωνία Πολυμεσικών Δεδομένων των UAV

Κωνσταντίνος Σιόντης

Α.Μ. 2016018026

Επιβλέπων καθηγητής

Ν. Δούκας

Αθήνα 2020

Πίνακας περιεχομένων

Πίνακας εικόνων

Περίληψη

Τα τελευταία χρόνια παρατηρείται αυξανόμενη χρήση μη επανδρωμένων οχημάτων (drones) σε εφαρμογές όπως ερευνητικές, στρατιωτικές και αστυνόμευσης. Η αύξηση της χρήσης των drones σε διάφορους τομείς φέρνει στο προσκήνιο άγνωστα έως τώρα κενά ασφαλείας ή αδυναμίες οι οποίες δεν θεωρούνταν ότι επιτρέπουν την εμφάνιση σημαντικών απειλών. Η εργασία αυτή μελετά και αναλύει τους παράγοντες κινδύνου και προτείνει λύσεις για συγκεκριμένα κενά ασφαλείας, στον τομέα της κρυπτασφάλειας.

Σύμφωνα με τη βιβλιογραφική ανασκόπηση των Krishna και Murphy (2017), υπάρχουν δυο βασικές κατηγορίες στις οποίες διακρίνονται οι κυβερνοεπιθέσεις σε μη επανδρωμένα οχήματα. Αυτές είναι οι *επιθέσεις διανύσματος (attack vector)* και *επιθέσεις στόχου (attack target).* Ειδικότερα οι επιθέσεις στόχου περιλαμβάνουν τις επιθέσεις σε GPS, στο κανάλι ελέγχου επικοινωνίας και στα δεδομένα επικοινωνίας (π.χ. η υποκλοπή δεδομένων και η αδυναμία παρουσίασης βίντεο στο χειριστή). Οι συνήθεις προσεγγίσεις δίνουν έμφαση στην επικοινωνία ελέγχου, ενώ εξακολουθούν να υφίστανται κενά ασφαλείας με επιπτώσεις στην ομαλή μετάδοση των δεδομένων.

Η παρούσα εργασία παρουσιάζει τα βασικά μέρη των UAV καθώς και τις κατηγοριοποιήσεις τους, συνεχίζει με τα προβλήματα κυβερνοασφάλειάς τους και εστιάσει στην μελέτη των επιθέσεων στο κανάλι της επικοινωνίας των δεδομένων και στις τεχνικές προστασίας κυβερνοεπιθέσεων αυτού του είδους με τους αλγορίθμους κωδικοποίησης πολυμεσικών δεδομένων. Επίσης, παρουσιάζει τη σχεδίαση, ανάπτυξη και δοκιμή αλγορίθμου για την κρυπτασφάλιση των πολυμεσικών δεδομένων ελέγχοντας για το αποδοτικότερο τύπο τους (format) και παρουσιάζει τα αποτελέσματα.

1. Εισαγωγή

Η χρήση μη επανδρωμένων αεροσκαφών (UAV) για παρακολούθηση και αναγνώριση είναι μια συνηθισμένη εφαρμογή της τεχνολογίας. Η πλειοψηφία των UAV, που χρησιμοποιούνται αποκλειστικά για αποστολές παρακολούθησης και αναγνώρισης, καλύπτει ένα ευρύτατο φάσμα από το Global Hawk, με άνοιγμα φτερών μεγαλύτερο από ενός Boeing 737 ως νανο-ελικόπτερα που ζυγίζουν λίγα γραμμάρια, όπως το Black Hornet 3 με μόλις 32 γραμμάρια, προσφέρει το χαμηλότερο μέγεθος, βάρος και απόδοση για UAV, ενώ πετά 2 χιλιόμετρα με ταχύτητες άνω των 21 χιλιομέτρων την ώρα. Επίσης, το Hornet 3 ενσωματώνει ευκρινή απεικόνιση με τη θερμική μικροκάμερα και κρυπτογραφημένο για στρατιωτικούς σκοπούς Data-Link, επιτρέποντας απρόσκοπτη επικοινωνία και εικόνες σημαντικά πέρα από το οπτικό πεδίο και στο κλειστές περιοχές (Nichols et al., 2018).

Εικόνα 1 Global Hawk (wiki)

Εικόνα 2 Black hornet 3 (Mohan, 2016)

Ένα UAV είναι απλά ο φορέας για το σύστημα αισθητήρων και ο εργαλείο που χρησιμοποιείται για την κίνηση και τον έλεγχο του αισθητήρα στον αέρα (Nichols et al., 2018). Με μια τόσο μεγάλη ποικιλία διαθέσιμων φορέων σήμερα, μπορεί να φορτωθεί ότι είδος αισθητήρα επιθυμεί ο χρήστης (πρβ ενότητα 3.2 κάμερες). Με αυτό τον τρόπο μπορούμε να επιχειρούμε σε άγνωστες και επικίνδυνες περιοχές, χωρίς να κινδυνεύουν ανθρώπινες ζωές. Επίσης, τα UAV δεν πάσχουν από κόπωση, δεν χάνουν την εστίαση και απαιτούν λιγότερη εκπαίδευση σε σύγκριση με τα επανδρωμένα αεροσκάφη. Οι τακτικές και οι τεχνικές που εφαρμόζονται στη σημερινή τεχνολογία προέρχονται από το πεδίο της τηλεπισκόπησης. Η τηλεπισκόπηση έχει μακρά ιστορία καθώς ξεκίνησε με τους ανθρώπους να προσπαθούν να δουν από απόσταση με τη χρήση περιστεριών σε μπαλόνια έως δορυφόρους. Αυτές ακριβώς οι

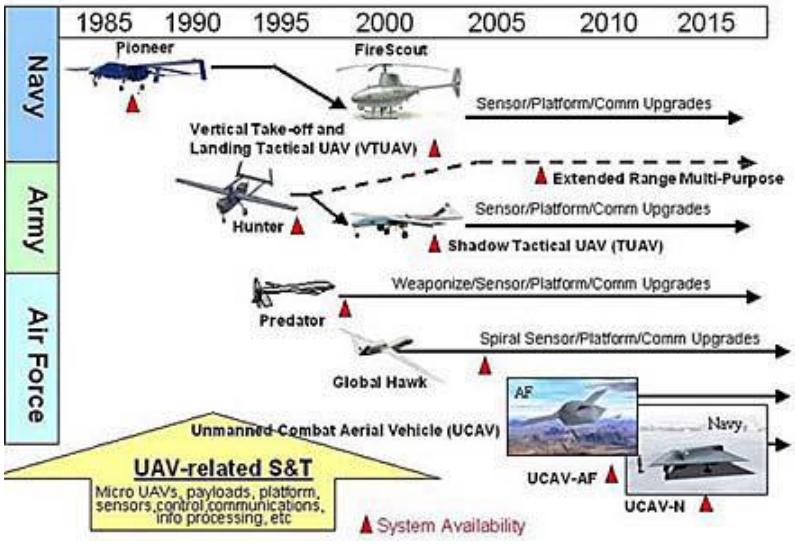
τακτικές αξιοποιήθηκαν στο έπακρο για στρατιωτικούς λόγους (επίθεση ή υπεράσπιση) καθώς και για την προστασία των πολιτών.

Πρώτος ο Ναπολέοντας και έπειτα οι επιτελείς του αμερικανικού εμφύλιου χρησιμοποίησαν μπαλόνια παρατήρησης για την παρακολούθηση των εχθρικών δραστηριοτήτων. Μόλις η μεθοδολογία λήψης φωτογραφίας και μαγνητοσκόπησης βελτιώθηκε και μπόρεσε να αποτυπώσει τη φωτογραφία σε φίλμ σε λιγότερες ώρες, έγιναν οι πρώτες αεροφωτογραφήσεις συνήθως με χαρταετούς και μπαλόνια. Ο πρώτος Αμερικανός που έβγαλε αεροφωτογραφίες ήταν ο Τζέιμς Γουάλας Μπλακ και φωτογράφησε το λιμάνι της Βοστώνης το 1860.

Εικόνα 3. Η πρώτη αεροφωτογραφία, το λιμάνι της Βοστόνης (Schultz, C. 2013)

Κατά τους Lillestand, Keifer και Chipman (2014; Nichols, 2018) η τηλεπισκόπηση ορίζεται ως η επιστήμη και η τέχνη της γνωριμίας ενός αντικειμένου, περιοχής ή φαινομένου μέσω της ανάλυσης της κατάστασης που αποκτήθηκε από μια συσκευή που δεν έρχεται σε επαφή με το υπό διερεύνηση αντικείμενο, περιοχή ή φαινόμενο. Με απλά λόγια είναι η μελέτη διαφορετικών σημείων ενδιαφέροντος από μακριά χωρίς να χρειάζεται δειγματοληψία που συνήθως γίνεται από αεροσκάφη επανδρωμένα ή μη.

Τα στρατιωτικά drones ανάλογα με το αν επιχειρούν στη ξηρά ή τη θάλασσα (Εικόνα 4) χρησιμοποιούνται για συνοριακή περιπολία και παρακολούθηση, για στρατιωτική παρακολούθηση λιμένων και εσωτερικής δραστηριότητας για εθνική ασφάλεια, για υποστήριξη επίγειων στρατευμάτων, για ανακάλυψη κόμβου και δικτύου, για παρακολούθηση αποστολής, για εκτίμηση ζημιών και για αποτροπή κίνησης.



Εικόνα 4. Η εξέλιξη των UAV Βιβλιοθήκη του Louisville. (2018)

Ο Ελληνικός Στρατός έχει ήδη ξεκινήσει τη χρήση drones (κυρίως της DJI) και η τρέχουσα πρακτική είναι η τοποθέτηση της κονσόλας χειρισμού σε οχήματα τύπου M/S 290 GDT ¼, χωρίς ακόμα να έχει καθοριστεί και τυποποιηθεί το πρωτόκολλο κρυπτασφάλισης των μεταδιδόμενων δεδομένων από τα drones στα οχήματα. Αντιθέτως, σε άλλα drones της στρατιωτικής και πολιτικής βιομηχανίας, η κρυπτασφάλιση δεν αποτελεί μέρος του αρχικού συνδυασμού, αλλά επέρχεται αργότερα ως development kit, παραγνωρίζοντας έτσι την ιδιαίτερα σημαντική παράμετρο της ασφαλούς μετάδοσης των πολυμεσικών δεδομένων. Γιαυτό το λόγο, η παρούσα εργασία εστιάζει στο πρόβλημα της κρυπτογράφησης πολυμεσικών δεδομένων κατά τη μετάδοση από το UAV προς τη βάση. Στην αρχή, αναλύονται τα τηλεπικοινωνιακά μέρη των UAV, όπως η ζεύξη δεδομένων, η διεπαφή του συστήματος και οι αισθητήρες, ενώ συνεχίζει με την ανάδειξη των επιθέσεων λόγω μη επαρκούς κρυπτογράφησης σήματος. Διαχωρίζει τις επιθέσεις σε φυσικές και λογικές, αναφέρεται στα είδη των λογικών επιθέσεων και τους τρόπους αποφυγής τους. Ταξινομεί και αναλύει αλγορίθμους κρυπτογράφησης πολυμεσικών δεδομένων σε πραγματικό χρόνο, ενώ επιλέγει έναν αλγόριθμο με πρώτιστο κριτήριο την ασφάλεια και στη συνέχεια την υπολογιστική ισχύ. Αυτόν τον αλγόριθμο, τον ελέγχει ως προς την αποτελεσματικότητά του, καθώς και ως προς την πιθανή διαφοροποίηση ανάλογα με το format του αρχικού βίντεο. Επιλέχθηκαν οκτώ διαδεδομένα formats (mp4, mpg, wmv, 3pg, mkv, avi, flv, f4v) τα οποία ελέγχθηκαν ως προς τον χρόνο κρυπτογράφησης και αποκρυπτογράφησης, τον ρυθμό μετάδοσης και το Peak Signal-to-Noise Ratio τόσο του αρχικού και του αποκρυπτογραφημένου βίντεο, όσο και μεταξύ των αρχικών βίντεο των διαφορετικών formats, ώστε έχουμε αποδεκτή ποιότητα και λιγότερα δεδομένα προς κρυπτογράφηση.

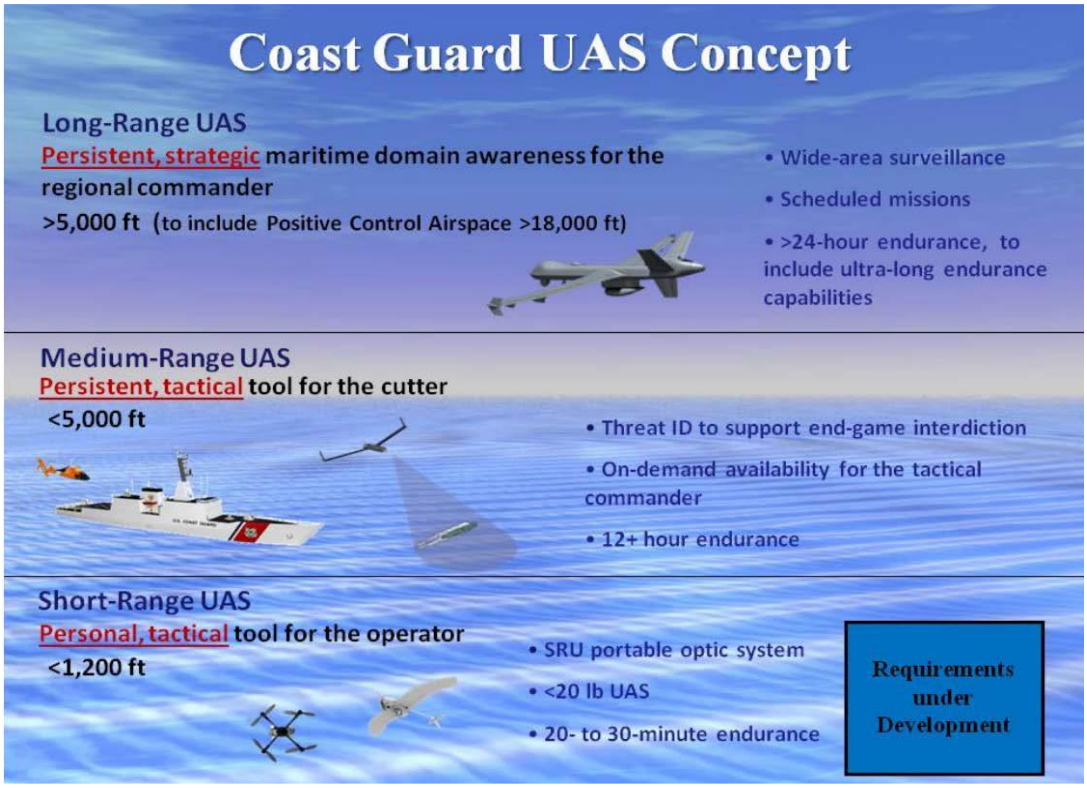
2. Κατηγοριοποίηση των UAV

Τα drones χωρίζονται συχνότερα σε τρεις κατηγορίες με βάση τη διάρκεια και τη λειτουργία της αποστολής τους (εικόνα 5, Nichols et al., 2018)

1. Υψηλού υψόμετρου και μεγάλης αντοχής, που χρησιμοποιείται συχνότερα για αναγνώριση, παρακολούθηση ή επίθεση

2. Μεσαίου υψομέτρου με μέτριο εύρος που χρησιμοποιείται συχνότερα για αναγνώριση και μάχη

3.



Εικόνα 5. Οι τρεις κατηγορίες UAV για θαλάσσια επιτήρηση (Haring, 2018)

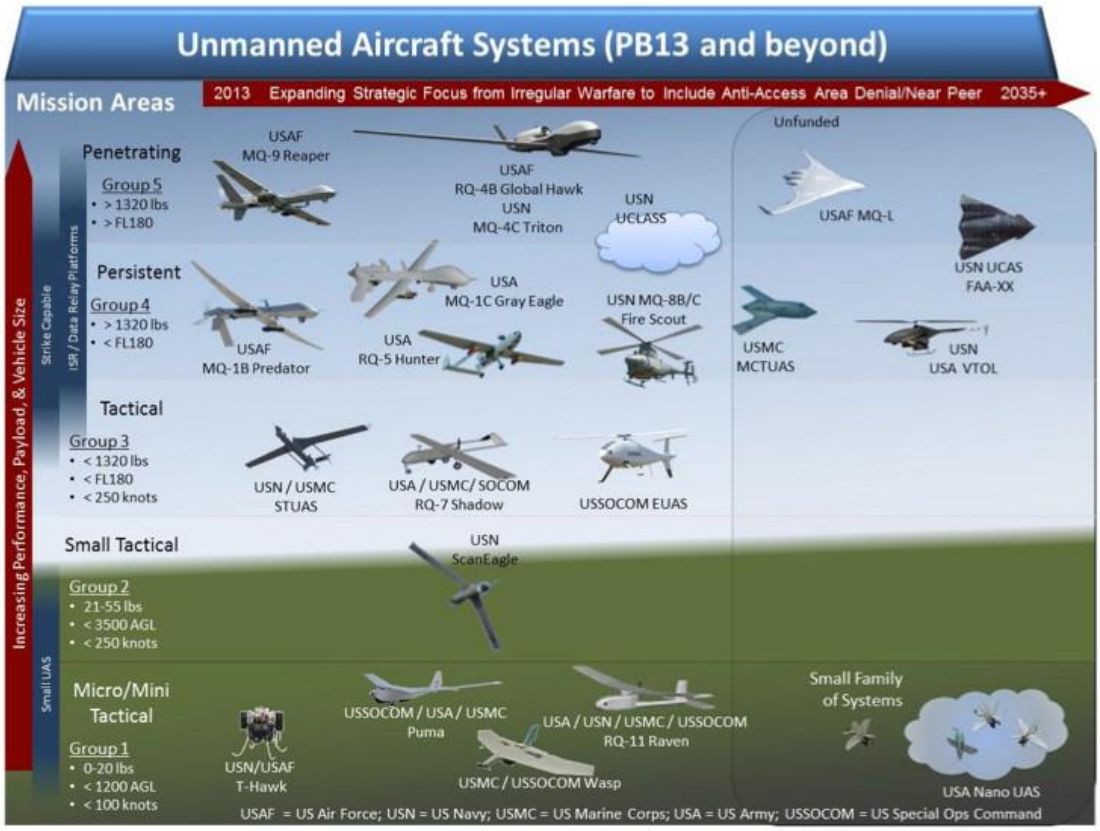
Άλλη κατηγοριοποίηση κατά ΝΑΤΟ (Αναδιώτης, 2018)
είναι η ακόλουθη:
Σύμφωνα με τη STANAG 4670 τα UAV37 μπορούν να κατηγοριοποιηθούν στις ακόλουθες γενικές Κατηγορίες:

1. Κλάσης I (Class I) με Μικτό Βάρος Απογείωσης < 150Kgr που περιλαμβάνει τις Κατηγορίες

   a. Small (Βάρος >15 Kgr, ύψος πτήσης ως τα 5000ft, δράση εντός οπτικής επαφής περίπου ως τα 50KM),
   b. Mini (Βάρος <15 Kgr, ύψος πτήσης ως τα 3000ft, δράση εντός οπτικής επαφής περίπου ως τα 25Km),
   c. Micro(Βάρος <15 Kgr, ύψος πτήσης ως τα 200ft δράση εντός οπτικής επαφής περίπου ως τα 5Km).

2. Κλάσης II (Class II) με Μικτό Βάρος Απογείωσης από 150 έως 600Kgr, με δυνατότητα δράσης εντός οπτικής επαφής με τον Σταθμό Εδάφους (LOS-Line Of Sight), επιχειρησιακή οροφή ως τα 18000ft.
3. Κλάσης III (Class III) με Μικτό Βάρος Απογείωσης > 600Kgr, δυνατότητα ακτίνας δράσης εκτός οπτικής επαφής με τον Σταθμό Εδάφους (BLOS-Beyond Line Of Sight) και χωρίζονται στην υποκατηγορία κατηγορία HALE (High Altitude Long Endurance) με δυνατότητα πτήσης (επιχειρησιακή οροφή) μέχρι 65000ft και κατηγορία MALE (Medium Altitude Long Endurance) μέχρι αντίστοιχα τα 45000ft.
4. Μικρό UAV μικρού κόστους και μικρής εμβέλειας (εικόνα 6)

Εικόνα 6. Hero 3 micro drone που εκτοξεύεται από στρατιώτη (Mohan, 2016)



Εικόνα 7. Μικρά και μίνι Drones (Jang, 2017)

3. Τηλεπικοινωνιακά μέρη του UAV

3.1 Η ζεύξη δεδομένων (Data-Link) και οι λειτουργίες της

Η Ζεύξη Δεδομένων (Data-Link) είναι ουσιαστικά το νευρικό σύστημα του UAV. Μεταδίδει δεδομένα εκ μέρους του χειριστή στο UAV είτε απευθείας μέσω οπτικής επαφής, ραδιοεπικοινωνίας από τον επίγειο σταθμό, είτε έμμεσα μέσω δορυφόρου ή βάσει υπολογιστικού νέφους δικτύων πολλαπλών UAV.

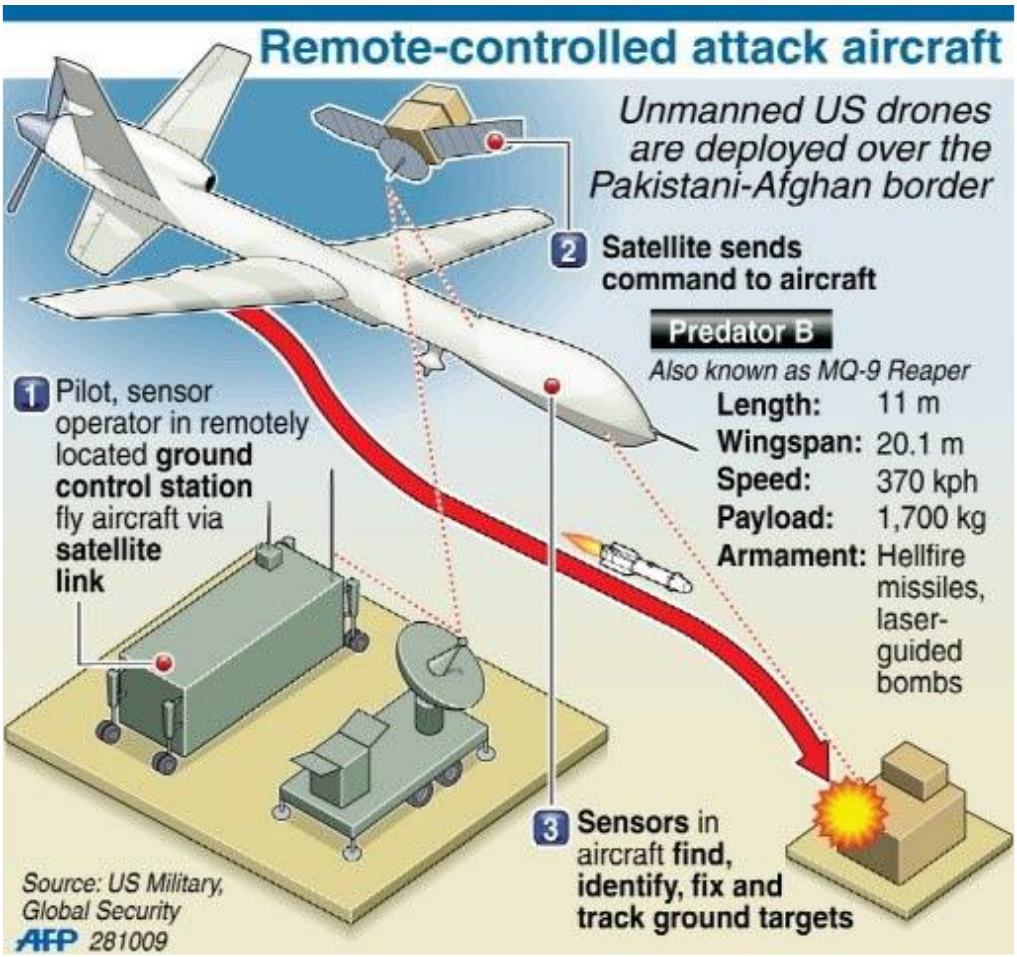
Υπάρχουν τέσσερις βασικές λειτουργίες επικοινωνίας και επεξεργασίας δεδομένων που το UAV πρέπει να μπορεί να είναι αποτελεσματικά και πραγματοποιεί αποτελεσματικά. Αυτές οι λειτουργίες είναι ζωτικής σημασίας για την ικανότητα του απομακρυσμένου χειρισμού ή του αυτόματου πιλότου για την άμεση έκδοση μιας εντολής, την επεξεργασία και την εκτέλεση (Nichols, et al., 2018).

- Το σύστημα βάσης UAV που υποστηρίζει τη διμερή επικοινωνία μεταξύ του UAV και του σταθμού εδάφους, παρέχοντας δεδομένα αισθητήρα στον χειριστή επιβεβαιώνοντας ότι η εντολή εκτελέστηκε
- Σύστημα αισθητήρων UAV, το οποίο σε στρατιωτικές εφαρμογές περιλαμβάνει κάμερες, GPS και ραντάρ, όπου τα δεδομένα συλλέγονται και υποβάλλονται

σε επεξεργασία από τους αισθητήρες και το βασικό σύστημα και στη συνέχεια κοινοποιείται στη βάση.

- Σύστημα Πλοήγησης UAV. Στο οποίο υπάγονται ηλεκτρονικές λειτουργίες UAV, όπως λειτουργία κινητήρα, πτερύγια, πηδάλια, αεροτομές και σταθεροποιητές, καθώς και ανταπόκριση στον χειριστή μετά την εκτέλεση της εντολής.
- Επικοινωνία κατά την πτήση, πάντα ασύρματα μεταξύ των επίγειων σταθμών μέσω γραμμής τοποθεσίας ή έμμεσης επικοινωνίας μέσω δορυφόρου (Hartman, 2013). Αυτό το τμήμα είναι το κύριο ενδιαφέρον της παρούσας εργασίας, γιατί, όπως θα δούμε μόνο η ασφαλής επικοινωνία με τη βάση εξασφαλίζει την καλή λειτουργία του UAV (τόσο ως προς την πλοήγηση, όσο και ως προς την αποστολή δεδομένων).

Ανεξάρτητα από την κατηγορία UAV, πρέπει τουλάχιστον αυτό να έχει τη δυνατότητα να συνεχίζει τη λειτουργία του ακόμη και όταν είναι πολύ μακριά από τον χειριστή για να το ελέγξει. Πρέπει υπάρχει η δυνατότητα αποστολής εντολών στο UAV ασύρματα και το UAV με τη σειρά του, πρέπει να είναι σε θέση να μεταδίδει δεδομένα, αποτελέσματα επεξεργασίας και δεδομένα αισθητήρων μετάδοσης. Τα δεδομένα πρέπει να είναι ασφαλή και να μεταδοθούν ασφαλώς μέσω ασύρματης επικοινωνίας ραδιοσυχνοτήτων. Κατά το σχεδιασμό, την ανάπτυξη και την του UAS, υπάρχουν πολλά ζητήματα που είναι ζωτικής σημασίας για μία επιτυχημένη και ισχυρή ανάπτυξη μιας δεδομένης εφαρμογής. Στον πυρήνα του είναι ένα μη επανδρωμένο σύστημα σχεδιασμένο να λειτουργεί απομακρυσμένα από έναν πιλότο που βρίσκεται λίγα μέτρα ή όπως σε στρατιωτικές εφαρμογές χιλιάδες μίλια μακριά.



Εικόνα 8. Παράδειγμα επίθεσης μέσω τηλεχειρισμού. Deadliest Unmanned Killing Machines in USA. (2011)

Η Ζεύξη Δεδομένων είναι ο δίαυλος με τον οποίο το UAV επικοινωνεί με τον σταθμό εδάφους και τον χειριστή καθώς ο τελευταίος στέλνει εντολές στο UAV για τον έλεγχο της αποστολής του, αξιολογεί τις μεταβαλλόμενες απειλές, την πλοήγηση, την ανταπόκριση σχετικά με το έδαφος και τις ατμοσφαιρικές συνθήκες κατά τη διάρκεια της αποστολής, καθώς και έλεγχο συλλογής πληροφοριών και σε στρατιωτικές εφαρμογές, παράδοση επιχειρησιακού φορτίου.

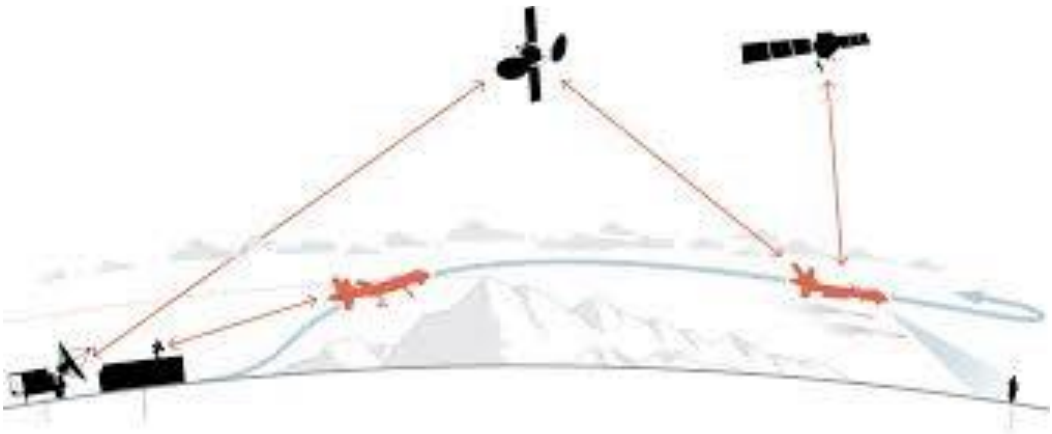
Οι προκλήσεις που παρουσιάζονται στον σχεδιαστή UAS είναι πολλές, ειδικά όταν πρόκειται για μεγιστοποίηση της ισχύος σήματος Data-Link με ταυτόχρονη διατήρηση της ασφάλειας των δεδομένων που μεταδίδονται και προστασία από πιθανά αντίμετρα και απειλές, ενδεικτικά, την παρεμβολή δεδομένων (Data Jamming), δεδομένων ή εξαπάτησης σήματος και αντι-ακτινοβολίας.

Βασικές λειτουργίες που απαιτούνται από το σύστημα επικοινωνίας UAV Data-Link είναι:

1. Ένας σταθμός εδάφους από τον οποίο ο χειριστής μπορεί να επικοινωνεί μέσω ραδιοφωνικής ζεύξης που επιτρέπει στο χειριστή τον έλεγχο του UAV, όσον αφορά την πλοήγηση και την ανάπτυξη ωφέλιμου φορτίου.

2. Μια κατερχόμενη ζεύξη (downlink) που χρησιμοποιείται για την αναμετάδοση δεδομένων αισθητήρων και ηλεκτρονικών δεδομένων από το UAV στον σταθμό εδάφους και στον χειριστή του UAS.
3. Αμφίδρομη επικοινωνία σχετικά με την απόσταση και το αζιμούθιο του UAV για να βοηθήσει με ακρίβεια την πλοήγηση και στόχευση (Fahlstrom, 2012).

Επιπλέον, το Data-Link πρέπει να έχει σχεδιαστεί για απρόσκοπτη διασύνδεση με συστήματα επί του UAV μέσω του Air Data Terminal (ADT) και των σχετικών συστοιχιών κεραιών που απαιτούνται για τη λήψη ραδιοφωνικών σημάτων από τον σταθμό εδάφους ή τα δορυφορικά σήματα αναμετάδοσης σε UAS που λειτουργούν σε σχέδια UAV πέρα από την οπτική γωνία. Μόλις ληφθούν από το ADT τα δεδομένα πρέπει στη συνέχεια να υποβληθούν σε επεξεργασία, μερικές φορές να συμπιεστούν και στη συνέχεια αμέσως να μεταδοθούν στα κατάλληλα υποσυστήματα του UAV όπως πλοήγηση, επίπεδο πτήσης, λειτουργία κινητήρα και στόχευση. Ομοίως, ο σταθμός εδάφους πρέπει επίσης να έχει τις ίδιες ικανότητες να λαμβάνει δεδομένα κατερχόμενης ζεύξης από το UAV. Μόλις ληφθούν τα δεδομένα κατερχόμενης ζεύξης πρέπει να υποβληθούν σε επεξεργασία, ενδεχομένως να συμπιεστούν ή να μετατραπούν, και στη συνέχεια να προωθηθούν στα κατάλληλα συστήματα, αισθητήρες, οθόνες ή βάσεις δεδομένων στο σταθμό εδάφους. Ανεξάρτητα από τη μέθοδο μετάδοσης των σημάτων ανερχόμενης ζεύξης ή τη ραδιοσυχνότητα («RF») τα σήματα διαφορετικών συχνοτήτων συνήθως διασφαλίζονται με τεχνικές διασποράς. (Kakar, 2017; Nichols et al., 2018).

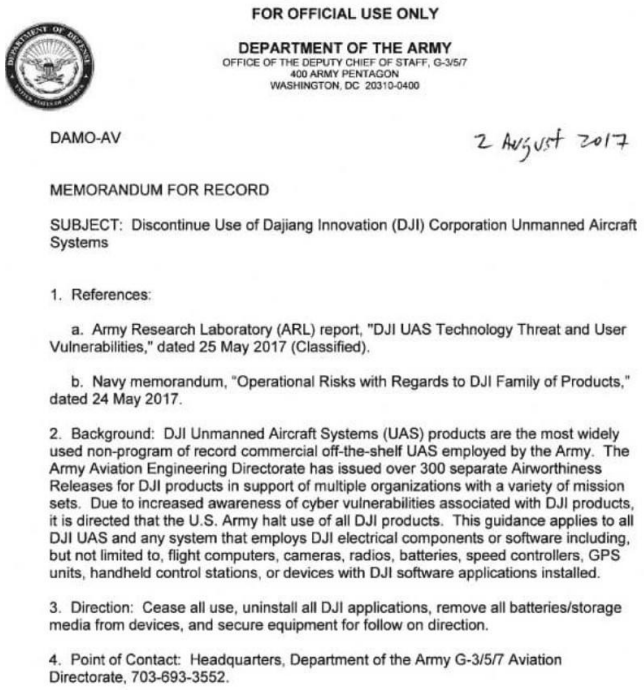


Εικόνα 9 Data-Link, από τη βάση, στον δορυφόρο και το UAV (Whitlock, 2014).

3.1.1 Είδος σημάτων

Τα αναλογικά σήματα είναι είδος σημάτων τα οποία σε γενικές γραμμές καθυστερούν σε σχέση με τα ψηφιακά, επειδή ταξιδεύουν με την ταχύτητα του φωτός (Reid, 2017). Η εξέλιξη των ασύρματων Data-Link ευνοεί την ψηφιακή διαμόρφωση, γεγονός που

συνάδει με τα δεδομένα που συλλέγει και επεξεργάζεται τα οποία είτε είναι ψηφιακά είτε αναλογικά δεδομένα που μετατρέπονται σε ψηφιακά. Η επικοινωνία του Data-Link ευνοεί τη μετάδοση ψηφιακών δεδομένων λόγω του μεγαλύτερου περιθωρίου παρεμβολών και της ευκολίας διασύνδεσης μεταξύ των συστημάτων του UAV (Fahlstrom, 2012). Ως προς την ευκολία ιδιαίτερο ρόλο παίζει η ταχύτητα χειρισμού πολλαπλάσιων δεδομένων. Αλλά το μεγάλο μειονέκτημα είναι πως αν παραβιαστεί τότε θα εξαχθούν μαζικά μεγάλες ποσότητες ευαίσθητων δεδομένων. Τέτοιου είδους παραβίαση έγινε το 2017 με τα drones της DJI, κινεζικής κατασκευής, τα οποία χρησιμοποιούνται κατά κόρον και από τον ελληνικό στρατό, με αποτέλεσμα ο στρατός των ΗΠΑ να απαγορεύσει τους, όπως φαίνεται από τη προειδοποίηση (Εικόνα 10).
Οι κινέζοι έχοντας πρόσβαση στη διαχείριση του συστήματος μπόρεσαν να προκαλέσουν εσφαλμένη καθοδήγηση στα συστήματα και ταυτόχρονα ο πιο σημαντικός λόγος εσωτερικής απειλής ήταν πως θα μπορούσαν να εμπλακούν στην στη διαδικασία μετάδοσης με αποτέλεσμα το σύστημα να περιέχει κώδικα που επηρεάζει κρατικές κατευθύνσεις και προτεραιότητες (Κόλλια, 2017).



FOR OFFICIAL USE ONLY

DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF, G-3/5/7
400 ARMY PENTAGON
WASHINGTON, DC 20310-0400

DAMO-AV

2 August 2017

MEMORANDUM FOR RECORD

SUBJECT: Discontinue Use of Dajiang Innovation (DJI) Corporation Unmanned Aircraft Systems

1. References:

a. Army Research Laboratory (ARL) report, "DJI UAS Technology Threat and User Vulnerabilities," dated 25 May 2017 (Classified).

b. Navy memorandum, "Operational Risks with Regards to DJI Family of Products," dated 24 May 2017.

2. Background: DJI Unmanned Aircraft Systems (UAS) products are the most widely used non-program of record commercial off-the-shelf UAS employed by the Army. The Army Aviation Engineering Directorate has issued over 300 separate Airworthiness Releases for DJI products in support of multiple organizations with a variety of mission sets. Due to increased awareness of cyber vulnerabilities associated with DJI products, it is directed that the U.S. Army halt use of all DJI products. This guidance applies to all DJI UAS and any system that employs DJI electrical components or software including, but not limited to, flight computers, cameras, radios, batteries, speed controllers, GPS units, handheld control stations, or devices with DJI software applications installed.

3. Direction: Cease all use, uninstall all DJI applications, remove all batteries/storage media from devices, and secure equipment for follow on direction.

4. Point of Contact: Headquarters, Department of the Army G-3/5/7 Aviation Directorate, 703-693-3552.

Εικόνα 10. Επιστολή του DARPA να σταματήσει τη χρήση drones της DJI (Scott, 2017)

3.1.2 Η διεπαφή του συστήματος

Προκειμένου το Data-Link να είναι αποτελεσματικό πρέπει η μετάδοση να είναι ασφαλής και γρήγορη ως προς το downlinking των δεδομένων (αφού στην παρούσα εργασία αναλύεται μόνο η ασφάλεια στη λήψη πολυμεσικών δεδομένων και όχι στην αποστολή των εντολών από τη βάση στο UAV, όπως φαίνεται και στην Εικόνα 12,

σελ.16), ενώ το επιχειρησιακό φορτίο του πρέπει να είναι μπορεί να διασυνδέσει και να υποστηρίξει τις ακόλουθες λειτουργίες

- Τον έλεγχο του UAV, συμπεριλαμβανομένων των αισθητήρων και των όπλων
- Το επιχειρησιακό φορτίο (προϊόν και έλεγχο αυτού)
- Τα όπλα (συμβατικά και ηλεκτρονικά)
- Την αντίληψη της κατάστασης στην οποία βρίσκεται το επιχειρησιακό φορτίο κάθε στιγμή (Υπουργείο Άμυνας ΗΠΑ, 2005).

3.1.3 Καθυστέρηση στη διεπαφή

Ως καθυστέρηση ορίζεται το διάστημα μεταξύ του χρόνου επεξεργασίας δεδομένων και του μεταδιδόμενου σήματος και της λήψης του σήματος, το οποίο στη συνέχεια υποβάλλεται στον χειριστή προς επεξεργασία (Nichols et al.,2018) Όταν υπάρχει οπτική επαφή, η μετάδοση και λήψη είναι σχεδόν στιγμιαία λόγω της ταχύτητας του φωτός (επί περιπτώσεων ίδιας ταχύτητας ζεύξης σε οπτική και μη οπτική επαφή). Δυστυχώς η έλλειψη ορατότητας, η μεγάλη απόσταση, το δυσχερές φυσικό περιβάλλον με βλάστηση, ο καιρός, ακόμη και η πυκνότητα του αέρα και το έδαφος (Διεθνής Ένωση Τηλεπικοινωνιών, 2009) μπορούν να περιορίσουν σημαντικά την ακτίνα λειτουργίας του UAV.

Τα πτητικά χαρακτηριστικά και ειδικά η δυνατότητα ακτίνας δράσης εντός ή εκτός οπτικής επαφής (Line of Sight-LOS) αποτελεί βασικό παράγοντα κατηγοριοποίησης των UAV σύμφωνα με το NATO. Επί του παρόντος υπάρχουν 3 κλάσεις λειτουργίας LOS των UAV:

Χαμηλής αντοχής

Μεσαίας αντοχής και

Υψηλή (κατά Valavanis, 2013 ή μακράς κατά NATO) αντοχής.

- Χαμηλή αντοχή.

Το UAV λειτουργεί σχεδόν αποκλειστικά σε οπτική επαφή, συνήθως στη μπάντα C (3000 Mhz) με χαμηλή συχνότητα μεταξύ 3,7-4,2 GHz για download και 5.9-6.4 για uplink. Ο κύριος λόγος επιλογής της C είναι ότι τα σήματα χαμηλής συχνότητας είναι λιγότερο ευαίσθητα σε υποβάθμιση που σχετίζεται με τον καιρό.

- Μεσαία αντοχή

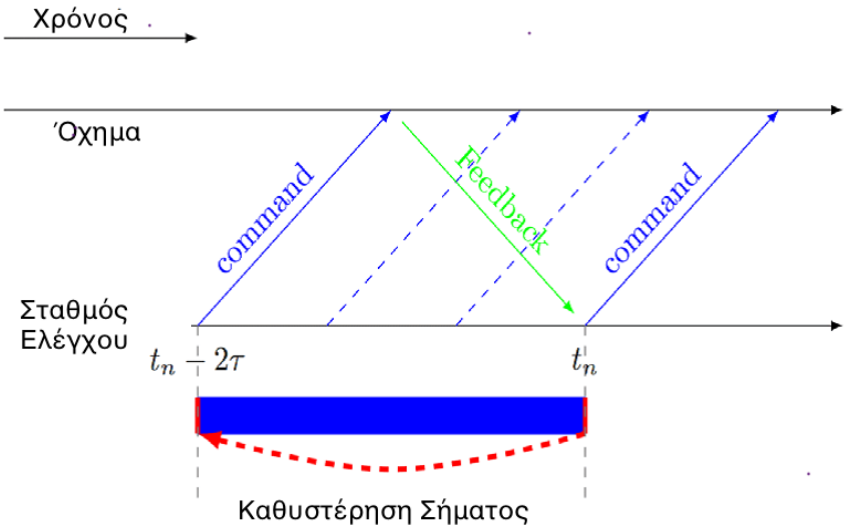
Λειτουργούν κυρίως σε οπτική επαφή (LOS), ωστόσο κάποια UAV έχουν δυνατότητα ακτίνας δράσης εκτός οπτικής επαφής (Beyond Line of Sight-BLOS). Όταν λειτουργούν σε αποστολές εντός οπτικής επαφής χρησιμοποιούν την μπάντα C, εάν όμως δρούν εκτός οτικής επαφής συνήθως λειτουργούν σε UHF (300 MHz) ως την

μπάντα Ku (15 GHz). Το downlink είναι μεταξύ 11,7 - 12,7 GHz και το uplink μεταξύ 14-14,5 GHz.

- Υψηλή αντοχή

Τα συγκεκριμένα drones έχουν ακτίνα δράσης εκτός οπτικής επαφής και εκπέμπουν σε UHF (300 MHz) ως σε μπάντα Ku (15 GHz). Η συχνότητα downlink κυμαίνεται μεταξύ 11,7 - 12,7 GHz και uplink μεταξύ 14-14,5 GHz. Επίσης, μπορούν να χρησιμοποιήσουν την τεχνολογία Common Data-Link ("CDL") είτε στη δορυφορική επικοινωνία στην μπάντα I είτε στη μπάντα Ku μεταξύ 14,5 και 15,38 GHz. Προκειμένου να ελαχιστοποιηθεί η καθυστέρηση του SATCOM ενεργοποιείται ο αυτόματος πιλότος όταν το UAV είναι εντός οπτικού πεδίου. (Valavanis, 2013).

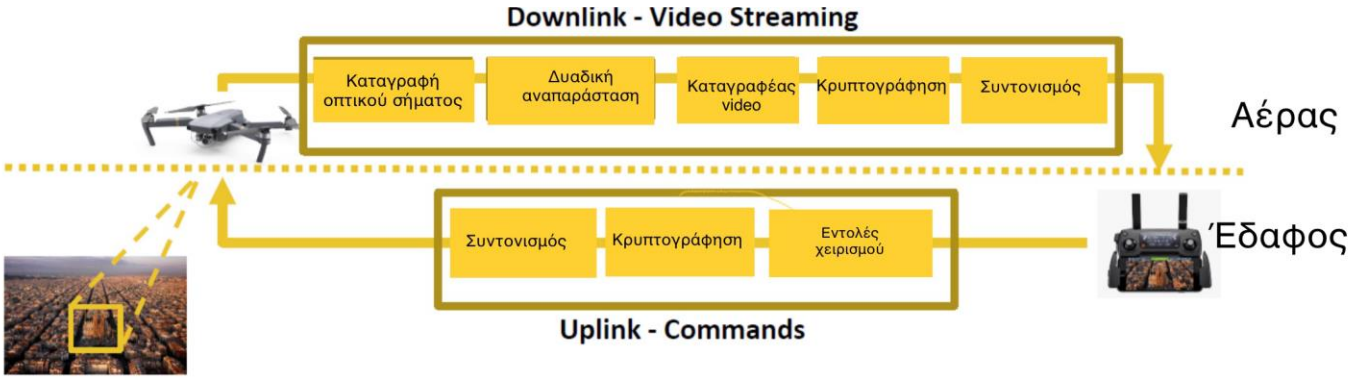
Το ισοζύγιο μεταξύ ασφάλειας και καθυστέρησης είναι δύσκολο να επιτευχθεί ακόμη και στα επανδρωμένα αεροσκάφη, τα οποία αντιμετωπίζουν καθυστέρηση πέντε ως οκτώ δευτερολέπτων στα χειριστήρια τους όταν πετούν εκτός οπτικής επαφής λόγω της κρυπτογράφησης και του χρόνου που απαιτείται για την αναμετάδοση εντολών μέσω δορυφόρων. Συνεπώς όσο ασφαλέστερη η επικοινωνία, τόσο μεγαλύτερη η καθυστέρηση. Παρ' ότι υπάρχουν επιλογές για να ελαχιστοποιηθεί η καθυστέρηση ενώ εξισορροπούνται τα επιμέρους χαρακτηριστικά που απαιτούνται για ένα ασφαλέστερο Data-Link των UAV, η καθυστέρηση είναι μια σταθερά υπαρκτή σε οποιαδήποτε μετάδοση, γιατί όσο μεγαλύτερη είναι η απόσταση, τόσο περισσότερος χρόνο χρειάζονται τα δεδομένα για να ταξιδέψουν, ενώ όσο μεγαλύτερο το επιχειρησιακό φορτίο των δεδομένων τόσο περισσότερος χρόνος απαιτείται για τη μετάδοση τους.



Εικόνα 11. Σχέση καθυστέρησης και ασφάλειας UAV Research Lab at the University of Sydney. (2018).

3.2 Αισθητήρες

Σε διάφορες περιπτώσεις χειρισμού των UAV (ειδικά των μικρότερων) υπάρχει δυο κανάλια επικοινωνίας που βασίζονται σε WiFi επικοινωνία και είναι σχεδιασμένα ώστε με το μεν πρώτο η κονσόλα ελέγχου να βλέπει σε πραγματικό χρόνο την κάμερα και το δεύτερο να πιλοτάρει το drone. Στην πραγματικότητα κάθε μικρό και μεσαίο UAV είναι μια ιπτάμενη κάμερα.



Εικόνα 12. Περιγραφή επικοινωνίας UAV με βάση (Netanel, 2020)

Οι πτήσεις των drones προορίζονται κυρίως για τη συλλογή δεδομένων. Τα δεδομένα που συλλέγονται μπορούν να χωριστούν σε δύο ευρείες κατηγορίες: in situ και τηλεσκοπικά (remote). Αυτές οι μέθοδοι χρησιμοποιούνται για τη συλλογή πληθώρας πληροφοριών, συμπεριλαμβανομένων των δυνάμεων ενός εχθρού και των πιθανών προθέσεων (Marshall, 2016; Nichols et al., 2018). Η in situ ανίχνευση σημαίνει ότι το αεροσκάφος μεταφέρεται στη θέση όπου πρέπει να γίνουν οι μετρήσεις. Στις περισσότερες περιπτώσεις ένα UAV πρέπει να ανταποκριθεί σε ένα ερέθισμα ή μια περιβαλλοντική παράμετρο, όπως είναι η μέτρηση ενός αερίου ή οι αλλαγές θερμοκρασίας.

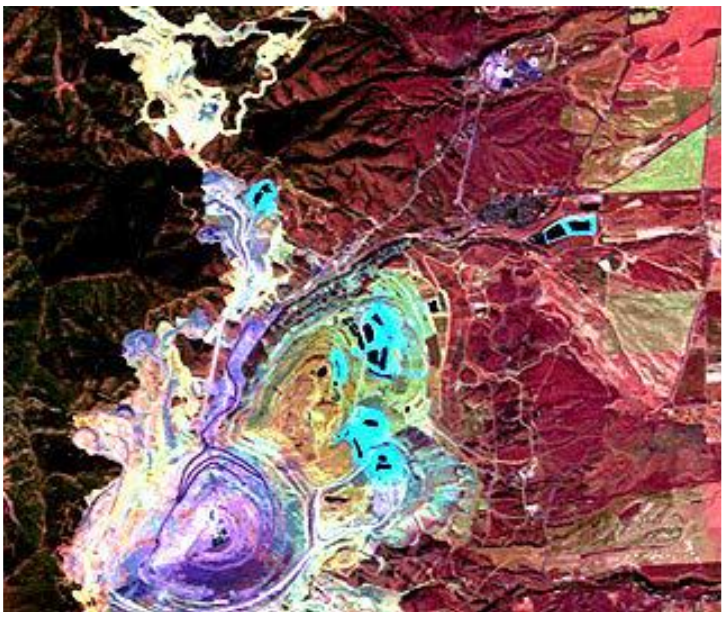
Η τηλεπισκόπηση είναι η διαδικασία ανίχνευσης ή μέτρησης ενός αντικειμένου ενδιαφέροντος από απόσταση, αλλά και των επιδράσεων του εν λόγω αντικειμένου, συνήθως με τη μορφή εκπεμπόμενων ή ανακλώμενων σωματιδίων ή / και κυμάτων. Υπάρχουν τρεις κατηγορίες τηλεπισκόπησης: επίγεια, αερομεταφερόμενη και διαστημική. Ενδιαφέρον της παρούσας εργασίας είναι η τηλεανίχνευση από αέρος (Airborne Remote Sensing, ARS) η οποία διαθέτει ένα ευρύ φάσμα επιλογών αισθητήρων, με κυρίαρχο την κάμερα. Υπάρχουν τέσσερις τύποι καμερών: ορατού φάσματος, εγγύς υπέρυθρων, υπέρυθρων και υπερφασματικές.

Οι κάμερες του ορατού φάσματος και των εγγύς υπέρυθρων λειτουργούν με τις ίδιες αρχές, με μοναδική διαφορά ότι ο αισθητήρας της δεύτερης περίπτωσης είναι ευαίσθητος στα μήκη κύματος κοντά στην υπεριώδη ακτινοβολία. Ενώ μια εικόνα του

ορατού αποτελείται από τρία κύρια χρώματα (κόκκινο, πράσινο, μπλε, RGB) οι εικόνες στο εγγύς υπεριώδες φως μπορούν να συλλάβουν πράσινο, κόκκινο και ένα ανακλαστικό χρώμα, το οποίο δεν είναι ορατό από το ανθρώπινο μάτι και συνθέτει το πρότυπο Color InfraRed. (Schowengerdt, 2007).

Εικόνα 13. Φωτογραφίες με κάμερα ορατού φωτός και υπερύθρων. (Young, 2018).

Οι κάμερες υπερύθρων (μεγάλου κύματος) ανταποκρίνονται στη θερμότητα που μετρούν οι αισθητήρες, αφού η αλλαγή θερμοκρασίας προκαλεί ένα ηλεκτρονικό σήμα. Οι υπέρυθροι αισθητήρες πέραν των 1800 nm έχουν διαφορετικές φυσικές και υλικές ιδιότητες από αυτών του ορατού. Τέλος οι υπερφασματικές κάμερες χρησιμοποιούν εκατοντάδες έγχρωμα κανάλια ανά εικόνα (όχι μόνο το μεμονωμένο κανάλι RGB). Η προκύπτουσα εικόνα ονομάζεται hyper cube και multi-band image, γιατί μοιάζει σαν να τραβάει πολλές φωτογραφίες τις οποίες ταυτόχρονα συγχωνεύει σε ένα τρισδιάστατο σύνολο δεδομένων που μπορεί να τεμαχιστεί για προβολή σε



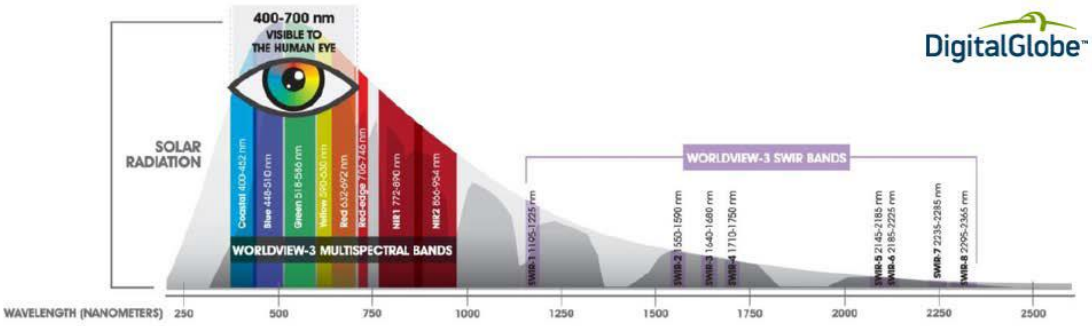
Εικόνα 14. Υπερφασματική φωτογραφία για την ανεύρεση και εξόρυξη πρώτων υλών (Hyperspectral Imaging, 2018)

πολλαπλές εικόνες με ξεχωριστά μήκη κύματος. Εάν το σύστημα καταγραφής ή το αντικείμενο κινείται, προστίθεται η τέταρτη διάσταση του χρόνου. Στην εικόνα 15 παρουσιάζεται μια φωτογραφία για επιχειρήσεις εξόρυξης της Αριζόνα που συλλαμβάνονται με την υπερφασματική απεικόνιση. Όμως, εκτός αυτής της περίπτωσης είναι δύσκολο να αναρτηθεί σε UAV λόγω της κατανάλωσης ισχύος, του βάρους, των δονήσεων, της απαίτησης για σταθερό σύστημα θέσης και προσανατολισμού και φυσικά λόγω υψηλού κόστους (Nichols et al., 2018).

Αναλυτικότερα για τις κάμερες του ορατού φωτός, των εγγύς υπερύθρων και των υπερύθρων (μεγάλου κύματος) μπορούν να βρίσκονται μαζί σε μια συσκευή καρδανικής ανάρτησης, η οποία επιτρέπει τη λειτουργία σε 360^{o}, γιατί μόνο έτσι επιτρέπεται η συνεχή παρατήρηση ενός επίγειου στόχου, ειδικά σε στρατιωτικές εφαρμογές. Η καρδανική ανάρτηση επιτρέπει την περιστροφή ενός αντικειμένου γύρω από έναν άξονα. Όταν υπάρχουν τρεις καρδανικές αναρτήσεις, η μια στερεώνεται πάνω στην άλλη, όπως γίνεται στα πλοία η στερέωση των γυροσκοπίων και των πυξίδων. Η ελληνική μετάφραση του ανωτέρω τρόπου ανάρτησης αναφέρεται στον Ιταλό μαθηματικό και φυσικό Gerolamo Cardano (1501–1576), ο οποίο ς την περιέγραψε, ενώ η πρώτη φορά που συναντάται είναι τον 3^{o} αιώνα π.Χ. σε κείμενο του Φίλωνα του Βυζάντιου (Wikipedia). Στην εικόνα 5 φαίνεται ένα σύστημα TASE 500 που λειτουργεί με κάμερες ορατού και υπερύθρων.

Εικόνα 15. TASE 500 που δουλεύει με κάμερες ορατού φωτός και υπερύθρων (Nichols et al., 2018)

Για την επιλογή της σωστής κάμερας, συνεκτιμώνται οι ιδιαίτερες ανάγκες κάθε αποστολής αλλά και της εκάστοτε πλατφόρμας, η οποία δημιουργεί τους συμβιβασμούς μεταξύ ενός αισθητήρα υψηλότερης ποιότητας που ζυγίζει περισσότερο και καταναλώνει ισχύ έναντι μιας κάμερας χαμηλότερης ποιότητας που είναι λιγότερο ακριβή και ελαφρύτερη, που όμως θα απαιτήσει περισσότερα περάσματα πάνω από το στόχο για τη λήψη χρήσιμων πληροφοριών, διαφορετικά θα παρέχουν ένα λιγότερο καθαρό σύνολο δεδομένων. Τα δεδομένα μπορούν να αυξήσουν το αποτύπωμα στον κυβερνοχώρο και να δημιουργήσουν περιττές ευπάθειες ως προς την κυβερνοασφάλεια.



Εικόνα 16. Ηλεκτρομαγνητικό φάσμα (Young, 2018)

Η τυπική κάμερα ενός drone είναι ένας παθητικός αισθητήρας που δεν εκπέμπει σήματα ή ενέργεια αλλά καταγράφει και στέλνει αυτά τα δεδομένα εξ ολοκλήρου σε παθητική λειτουργία. Συνηθισμένες περιπτώσεις καμερών προσφέρουν πολλές φιλικές προς το χρήστη δυνατότητες, όπως οι δημοφιλείς κάμερες Go-Pro που φαίνονται παρακάτω. Κατά τη διάρκεια της πτήσης μπορούν να στείλουν δεδομένα υψηλής ποιότητας σε ζωντανή ζεύξη για επεξεργασία στο έδαφος ή και να επεξεργαστούν πάνω στο UAV, όταν απαιτείται.

Πίνακας 1. Κάμερες ορατού φωτός και χαρακτηριστικά τους (GoPro, 2018)

χαρακτηριστικά	***Hero 5 Camera***	***Hero 5 Camera***	***Fusion Camera***
			
Φωτογραφική μηχανή	*12MP/30fps ρήξη*	*12MP/30fps ρήξη*	*18MP/30fps*
βίντεο	*4K30*	*4K60*	*5.2K30*
Σφαιρική λήψη	*όχι*	*όχι*	*ναι*
Αδιάβροχη	*10m*	*10m*	*5m*
Έλεγχος ήχου	*ναι*	*ναι*	*ναι*
Σταθεροποιητής βίντεο	*ναι*	*προηγμένη*	*προηγμένη*
Quick stories	*ναι*	*ναι*	*όχι*
HDR λήψη	*όχι*	*ναι*	*όχι*
Zoom αφής		*ναι*	*όχι*
Αυτόματος χαμηλός φωτισμός	*ναι*	*ναι*	*όχι*

Exposure control	*ναι*	*ναι*	*όχι*
Προηγμένη Μείωση θορύβου	*3-mic processing*	*3-mic processing*	*4-mic processing*
360	*όχι*	*όχι*	*ναι*
GPS	*ναι*	*ναι*	*ναι*
WiFi-διαμόρφωση	*ναι*	*ναι*	*ναι*
5 GHz WiFi για μεταφορά σε τηλέφωνο	*όχι*	*ναι*	*ναι*

4. Επίθεση – κρυπτογράφηση σήματος

Σύμφωνα με τον Han (2017), στον ηλεκτρονικό πόλεμο (electronic warfare) οι οντότητες που επηρεάζουν την ασφάλεια του συστήματος μπορούν να χωριστούν σε δύο τύπους: απειλές και επιθέσεις. Πιο συγκεκριμένα ως απειλή θεωρείται η πιθανότητα παραβίασης της ασφάλειας μιας οντότητας, περίστασης, ικανότητα, δράσης ή γεγονότος που θα μπορούσε να προκαλέσει βλάβη. Αντίθετα, ως επίθεση λογίζεται μια σκόπιμη πράξη κατά την οποία μια οντότητα επιχειρεί να αποφύγει τις υπηρεσίες ασφαλείας και παραβιάζει την πολιτική ασφαλείας ενός συστήματος. Πρόκειται είτε για μια πραγματική επίθεση στο σύστημα ασφάλειας είτε αναφέρεται σε μια μέθοδο που χρησιμοποιείται για να προσβάλει το σύστημα. Σκοπός μιας επίθεσης είναι να αλλάξει τους πόρους του συστήματος ή να επηρεάσει τη λειτουργία τους. Ειδικά σε ένα UAV, οι επιθέσεις περιλαμβάνουν τροποποιήσεις των δεδομένων ροής ή τη δημιουργία ψευδών ροών και μπορεί να χωριστεί σε τέσσερις κατηγορίες: πλαστογράφηση/μεταμφίεση, επανάληψη, τροποποίηση μηνυμάτων και άρνηση παροχής υπηρεσιών.

Στην πλαστογράφηση/μεταμφίεση ο εισβολέας επιτίθεται όταν μια οντότητα προσποιείται ότι είναι διαφορετική οντότητα, ενώ συνήθως περιλαμβάνει και μια από τις άλλες μορφές επίθεσης, όπως η ανίχνευση και η αναπαραγωγή ακολουθιών ελέγχου ταυτότητας μεταξύ UAV και σταθμών ελέγχου εδάφους, ώστε ο εισβολέας να αποκτήσουν πρόσβαση στο UAV, να παρεισφρήσουν στις επικοινωνίες και να αποστείλουν επιβλαβείς εντολές.

Η επανάληψη περιλαμβάνει την παθητική καταγραφή μιας ροής ελέγχου ταυτότητας ή μιας εντολής ροή ώστε ο εισβολέας να παραγάγει ένα μη εξουσιοδοτημένο αποτέλεσμα.

Η τροποποίηση των μηνυμάτων δηλώνει απλώς ότι ένα μέρος ενός νόμιμου μηνύματος τροποποιείται ή ότι τα μηνύματα καθυστερούν για την παραγωγή μη εξουσιοδοτημένου
αποτελέσματος.

Τέλος, μια επίθεση άρνησης υπηρεσίας αποτρέπει ή αναστέλλει την κανονική χρήση ή διαχείριση της επικοινωνίας. Αυτή η επίθεση έχει συνήθως έναν συγκεκριμένο στόχο, όπως το να καταστείλει όλα τα μηνύματα που κατευθύνονται σε ένα συγκεκριμένο drone και να το οδηγήσει σε προσγείωση. Μια άλλη μορφή άρνησης υπηρεσίας είναι η διακοπή ενός δικτύου είτε απενεργοποιώντας το είτε υπερφορτώνοντάς το με μηνύματα για να υποβαθμίσει την απόδοσή του. Αυτό το είδος επίθεσης στοχεύει στις ευαίσθητες πληροφορίες που μεταφέρονται μέσω του καναλιού επικοινωνίας, όπως

μηνύματα ελέγχου, μηνύματα ανταλλαγής κλειδιών, κ.α. Ωστόσο, λόγω της ποικιλίας των επιθέσεων, είναι δύσκολο στα συστήματα να αποτρέψουν τις επιθέσεις.

Οι κύριες μέθοδοι ασφαλείας στις επιθέσεις είναι ο έλεγχος ταυτότητας και της ασφάλειας συστήματος. Μια παθητική επίθεση προσπαθεί να μάθει ή να χρησιμοποιήσει πληροφορίες από ένα σύστημα αλλά δεν επηρεάζει τους πόρους του συστήματος. Οι παθητικές επιθέσεις είναι μια μορφή παρακολούθησης ή υποκλοπής των μεταδόσεων, όπου στόχος του αντιπάλου είναι να λάβει οποιαδήποτε πληροφορία μεταδίδεται. Οι παθητικές επιθέσεις διακρίνονται σε δύο τύπους: απελευθέρωση περιεχομένου μηνυμάτων και ανάλυση κυκλοφορίας. Η απελευθέρωση των περιεχομένων των μηνυμάτων γίνεται εύκολα κατανοητή όταν ένα μήνυμα μεταφοράς κλειδιού ή ένα μήνυμα ελέγχου UAV μπορεί να περιέχει εμπιστευτικές πληροφορίες τις οποίες οι χειριστές των UAV επιθυμούν να εμποδίσουν τον αντίπαλο να μάθει το περιεχόμενο αυτών των μεταδόσεων. Ο δεύτερος τύπος παθητικής επίθεσης, η ανάλυση κυκλοφορίας, είναι πιο σύνθετος. Ας υποθέσουμε ότι οι χειριστές των UAV θα μπορούσαν να κρυπτογραφήσουν το περιεχόμενο των μηνυμάτων μεταφοράς κλειδιών ή μηνυμάτων ελέγχου πτήσης έτσι ώστε ακόμα και αν οι εισβολείς καταγράψουν τα μηνύματα, δεν θα μπορούν να εξαγάγουν κανένα χρήσιμο περιεχόμενο.

4.1 Περιπτώσεις

4.1.1 Ανίχνευση υποκλοπής δεδομένων.

Τον Φεβρουάριο του 2016 οι Ισραηλινές αρχές συνέλαβαν έναν Παλαιστίνιο με την υπόνοια της υποκλοπής δεδομένων από Ισραηλινά drones (Nichols et al., 2018). Παρ' ότι οι λεπτομέρειες της υπόθεσης ήταν λιγοστές, φαίνεται ότι ο Majd Ouida, 22 ετών κατά την σύλληψή του, είχε καταφέρει να επιφέρει ρήγμα στην προστασία και τελικά να επιτύχει πρόσβαση στα δεδομένα παρακολούθησης των drone από το 2011 έως το 2014. Σε κάθε περίπτωση είχε συλλέξει τις εκπομπές τους χρησιμοποιώντας επιτρεπτές κεραίες και τεχνολογία επεξεργασίας, αφού επρόκειτο για μετάδοση. Όπως επεσήμανε ο David Axe, το εντυπωσιακό ήταν ότι οι Ισραηλινές αρχές τον συνέλαβαν κατηγορώντας τον ότι το διέπραξε ενώ δεν υπάρχει κανένας ξεκάθαρος τρόπος να γίνει αντιληπτό πότε κάποιος έχει υποκλέψει το βίντεο του drone. Το ερώτημα που ανακύπτει είναι πώς οι Ισραηλινοί γνώριζαν ότι τα δεδομένα είχαν περισυλλεγεί από μη εξουσιοδοτημένα άτομα; Πρόκειται για ένα κλασικό πρόβλημα ανίχνευσης εμπιστευτικότητας. Όταν έχει γίνει μια κλοπή σε φυσική μορφή, λείπει το φυσικό αντικείμενο. Αλλά όταν δημιουργείται ένα κρυφό αντίγραφο, ή υποκλέπτεται μια συνομιλία, δεν υπάρχει αδιαμφισβήτητος τρόπος να αποδείξει κανείς ότι το απόρρητό

έχει παραβιαστεί. Για παράδειγμα, αν ένας δυνητικός κλέφτης μπει στο κτίριο και τράβηξει μια φωτογραφία στρατηγικής σημασίας, ο ανταγωνιστής δεν θα μπορεί να αποδείξει ότι παραβιάστηκε το απόρρητο, παρά μόνο άν ήταν σε ισχύ οι δυνατότητες ανίχνευσης (π.χ. κάμερες παρακολούθησης), διαφορετικά μια τέτοια κλοπή θα μπορούσε να παραμείνει μη εντοπισμένη με απτά τεκμήρια.

Το πρώτο βήμα για να εντοπιστεί η παραβίαση εμπιστευτικότητας είναι ο προσδιορισμός του ποσοστού διακύβευσης του απόρρητου. Αυτό το σενάριο είναι που κάνει τις ασκήσεις επίθεσης / άμυνας να είναι πολύτιμες, ώστε να γίνει αντιληπτό πώς θα αποκτήσουμε πρόσβαση στις πληροφορίες που συλλέγονται από έναν αισθητήρα και θα αποκαλυφθούν ενδιαφέρουσες αδυναμίες και ευκαιρίες για τη δημιουργία λύσεων.

4.1.2 Όταν το UAV αγνοείται

Τα μη επανδρωμένα εναέρια συστήματα απαιτούν τον έλεγχο του συστήματος πλοήγησης μέσω συνδυασμού τηλεχειριστηρίου και αυτόνομης προεπιλογής. Σε περίπτωση απώλειας της απομακρυσμένης συνδεσιμότητας, το UAV διαθέτει συνήθως ένα σύνολο προεπιλεγμένων προγραμμάτων ασφαλούς προσγείωσης που συμμορφώνονται με το προφίλ αποστολής του.

Όταν ένα UAV αποστέλλεται σε εχθρική περιοχή είναι δεδομένο ότι ο αντίπαλος θα προσπαθήσει να το καταρρίψει. Ένας άλλος κίνδυνος είναι η εν όλω ή εν μέρει κατάληψη του UAV. Αυτό συνέβη τον Δεκέμβριο του 2011, όταν στην κατοχή του Ιράν περιήλθε drone επιτήρησης των ΗΠΑ. Επρόκειτο για ένα Lockheed Martin RQ-170 Sentinel που εκτελούσε αποστολή πάνω από το Αφγανιστάν κοντά στα ιρανικά σύνορα. Οι Ιρανοί αρχικά ισχυρίστηκαν ότι κατέλαβαν το RQ-170 μέσω κυβερνοεπίθεσης, ενώ αργότερα είπαν ότι ήταν σε θέση να αποκωδικοποιήσουν όλα τα αποθηκευμένα δεδομένα από τα συστήματα

Εικόνα 17. Επίδειξη του UAV από τις ιρανικές αρχές (Opall-Rome, 2018)

Έχουν γίνει διάφορες εικασίες για τις συνθήκες που έγινε η κατάληψη του UAV, τόσο από τις ΗΠΑ όσο και από το Ιράν. Πιθανές μέθοδοι μπορεί να ήταν η πλαστογράφηση του GPS, η παρεμβολή στο σύστημα ελέγχου και τέλος η φυσική ζημιά. Οι ΗΠΑ ζήτησαν την επιστροφή του RQ-170, ενώ το Ιράν αντέκρουσε αυτά τα αιτήματα ισχυριζόμενο ότι ο ιρανικός εναέριος χώρος είχε παραβιαστεί και αυτό συνιστά παραβίαση διεθνών κανόνων. Το 2016, το Ιράν ισχυρίστηκε ότι είχε αντιστρέψει τη σχεδίαση του RQ-170 δημιουργώντας την δική του έκδοση. Το γεγονός παρέμεινε στις ειδήσεις για αρκετά χρόνια. Τα αναπάντητα ερωτήματα, όμως, παραμένουν. Το αεροσκάφος απέτυχε ή καταρρίφθηκε σκόπιμα; Μια πιθανότητα είναι το RQ-170 να απέτυχε κατά την πτήση και να προσγειώθηκε σε μια περιοχή όπου οι Ιρανοί κατάφεραν να το ανακτήσουν πριν από τις φίλιες δυνάμεις. Θα μπορούσε να συμβεί μια σειρά από αστοχίες, όπως απώλεια του συστήματος τροφοδοσίας, παραβίαση των συστημάτων πλοήγησης ή κάποια φυσική ζημιά στο αεροσκάφος. Ένα προφανές ερώτημα που προκύπτει είναι, γιατί δεν ενσωματώθηκε δυνατότητα αυτοκαταστροφής. Σε τελική ανάλυση, σε περιπτώσεις πτήσης κοντά ή πάνω από εχθρική περιοχή, πρέπει να υπάρχει ένα σχέδιο για τον κίνδυνο σύλληψης. Το ιστορικό του U-2 που δοκιμάστηκε από τον Francis Gary Powers, και καταρρίφθηκε από τη Σοβιετική Ένωση το 1960, είχε τα χαρακτηριστικά γνωρίσματα της μυστικότητας (ακραίο υψόμετρο) και ο κίνδυνος θεωρήθηκε χαμηλός. Ακόμα κι έτσι όμως καταρριφθηκε. Ένα σύστημα αυτοκαταστροφής θα μπορούσε να ενεργοποιηθεί εξ αποστάσεως όταν έγινε αντιληπτό ότι το drone δεν ήταν σε φιλικό έλεγχο. Εναλλακτικά, ένας μηχανισμός

καταστροφής θα μπορούσε λογικά να ενεργοποιηθεί κατόπιν απώλειας σήματος ή όταν μεσολαβούσε μια εκτεταμένη περίοδος χωρίς εξουσιοδοτημένη επαφή.

Δεδομένου ότι κανένα σύστημα δεν είναι τέλειο, θα πρέπει να εξεταστούν εναλλακτικές λύσεις για μια τέτοια ικανότητα αυτοκαταστροφής. Για παράδειγμα, ένας μηχανισμός αυτοκαταστροφής (εκρηκτικό, οξύ κ.λπ.) θα μπορούσε να ενσωματωθεί στο προστατευτικό περίβλημα των συστημάτων, ενώ ο μηχανισμός ανίχνευσης θα μπορούσε να ενσωματωθεί στο ίδιο το περίβλημα με διάφορα μέσα. Εάν ανοίξει το περίβλημα, θα ήταν η σειρά της θήκης να καταστραφεί, με αυτόματη πυροδότηση. Σε αυτήν την περίπτωση, το αποτέλεσμα θα ήταν η καταστροφή δεδομένων ή / και εξοπλισμού. Ένα πραγματικό παράδειγμα αυτού του τύπου ολοκληρωμένης ικανότητας ανίχνευσης / αντίδρασης μπορεί να φανεί σε οποιοδήποτε μουσείο, όπου λεπτά πλέγματα καλωδίων ενσωματώνονται σε περιβλήματα, τα οποία, όταν χωρίζονται, ανοίγουν το ηλεκτρικό κύκλωμα και ενεργοποιείται ένας συναγερμός (Nichols et al., 2018).

4.2 Φυσικές και λογικές επιθέσεις

Σύμφωνα με τον Mohan (2016) ένα drone μπορεί να υποστεί επίθεση με δύο διαφορετικούς τρόπους: είτε με φυσική επίθεση, είτε με λογική επίθεση. Στο πρώτο είδος επίθεσης υπάρχει εμπλοκή με αεροσκάφος, πυροβολισμός με όπλο ενός drone, συντριβή ενός drone από ένα άλλο drone και σύλληψη ενός UAV με κάποιο άλλο φυσικό εξοπλισμό (π.χ γεράκια). Ο Peter Holley (2016), ένας δημοσιογράφος από την Washington Post έγραψε ότι η ολλανδική αστυνομία συνεργάστηκε με την Guard From Above, μια εταιρεία που ειδικεύεται στην εκπαίδευση αρπακτικών πτηνών, όπως αετών, εναντίον παράνομα εισερχομένων drone. Αυτά τα πουλιά αντιλαμβάνονται τα drone ως θήραμά τους, τους επιτίθενται και τα μεταφέρουν σε ασφαλές μέρος όπου δεν υπάρχουν άλλα πτηνά ή άνθρωποι.

Εικόνα 18. Εκπαιδευμένος αετός για να κατεβάζει drones (Holley, 2016)

Σύμφωνα με τον Rodday (2015), κατά τη λογική επίθεση, οι εισβολείς επιτίθενται σε drones μέσω ηλεκτρονικής παρεμβολής. Τα drones βασίζονται σε τεχνολογικά συστήματα για να επικοινωνούν με τον χειριστή και να καθορίζουν τις παραμέτρους πτήσης τους όπως ταχύτητα, υψόμετρο κ.λπ. Εάν επηρεαστούν αυτές οι παράμετροι από έναν επιτιθέμενο, τα drone θα υπακούσουν την εντολή του εισβολέα. Το καλύτερο παράδειγμα ενός λογικού φορέα επίθεσης είναι το DroneDefender που εφευρέθηκε από μια μη κερδοσκοπική εταιρεία με βάση το Οχάιο και την εταιρεία Battelle. Το DroneDefender (εικόνα 19) δημιουργεί βλάβη στο τηλεχειριστήριο και το GPS των drone έως 400 μέτρα, χωρίς παράπλευρη ζημιά (Battelle, 2016).

Εικόνα 19. DroneDefender (Battelle, 2016)

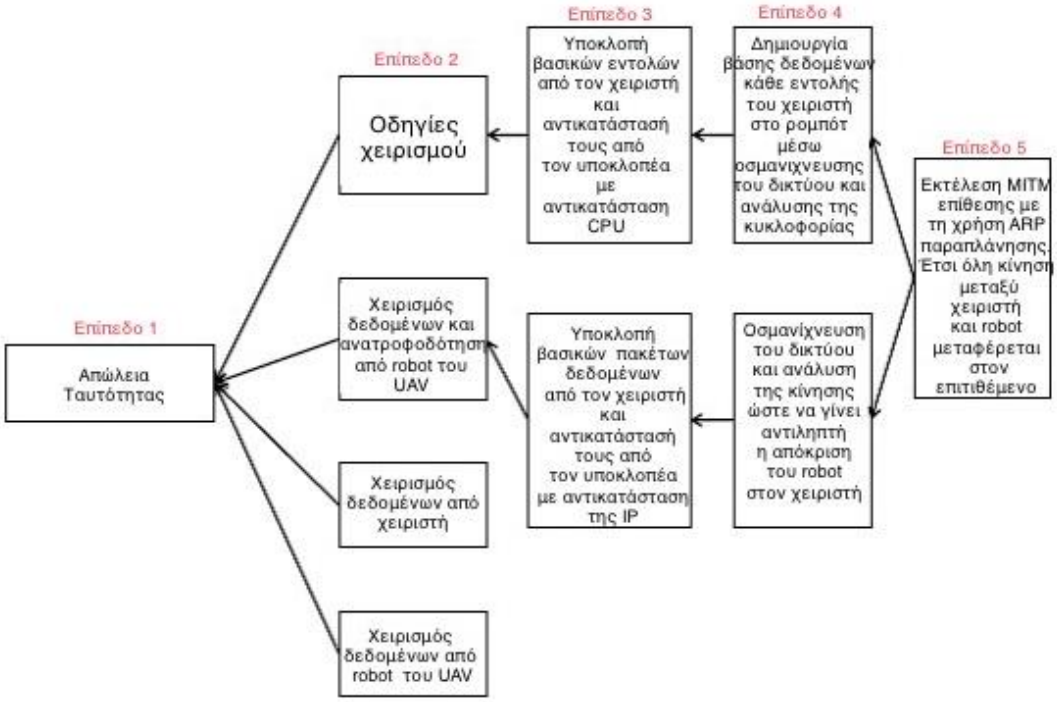
4.3 Προστασία των συστημάτων από λογικές επιθέσεις

Αισθητήρες, Data-Links, πλατφόρμες και τροφοδοτικά τείνουν να κατασκευάζονται ανεξάρτητα χωρίς πρότυπα προστασίας στον κυβερνοχώρο που δημιουργούνται αφήνοντας τα συστήματα ευάλωτα. Η ίδια η φύση του "plug and play" τείνει να δημιουργεί ασυμβατότητα στην προστασία στον κυβερνοχώρο.

Ανάλυση των παραμέτρων και των ελεγκτών πτήσης / μικροεπεξεργαστών πολλών δημοφιλών μοντέλων UAV που φέρουν πολλούς ρότορες αποκάλυψαν αδυναμίες που σχετίζονται τόσο με τη σύνδεση δεδομένων τηλεμετρίας όσο και με τη ροή δεδομένων από ένα drone μέσω συνδέσεων σειριακής θύρας (στις οποίες οι πληροφορίες θα μπορούσαν να ληφθούν ή να τροποποιηθούν) και τις συνδέσεις των UAV στη διεπαφή του επίγειου σταθμού τους (των οποίων η σύνδεση δεδομένων θα μπορούσε να πλαστογραφηθεί, επιτρέποντας σε εισβολείς να αναλάβουν τον πλήρη έλεγχο του οχήματος) (Nichols et al, 2018). Οι κίνδυνοι ασθενών πρωτοκόλλων ασφαλείας γίνονται ολοένα και πιο εμφανείς, όπως αναφέρθηκε από το CNN στις 17 Δεκεμβρίου του 2009 ότι οι αντάρτες μπόρεσαν να χρησιμοποιήσουν ένα πρόγραμμα λογισμικού μαζικής αγοράς για να δουν ζωντανές ροές από αμερικανικά στρατιωτικά αεροσκάφη Predator που παρακολουθούν στόχους στο Ιράκ. Υπάρχουν επίσης ενδείξεις ότι οι τροφοδοσίες UAV αποκτήθηκαν παράνομα από ιρανικές δυνάμεις στο Αφγανιστάν, αλλά δεν υπήρξαν αποδείξεις ότι οι μαχητές μπόρεσαν να πάρουν τον έλεγχο των drones και στις δύο χώρες. Το φθηνό λογισμικό, που δημιουργήθηκε από μια ρωσική εταιρεία επ' ονόματι SkyGrabber είναι διαθέσιμο από το Διαδίκτυο. Επιτρέπει στους χρήστες να επωφεληθούν από μη προστατευμένους συνδέσμους επικοινωνίας σε ορισμένα από τα UAV (Mount & Quijano, 2009).

Ένας εισβολέας μπορεί να έχει πολλούς στόχους για την έναρξη μιας επίθεσης. Πιθανοί στόχοι περιλαμβάνουν την απώλεια δεδομένων, τη σύνδεση με το UAV ή το επιχειρησιακό φορτίο. Ένα παράδειγμα σχεδιαγραμματικής απεικόνισης των επιθέσεων που βασίζονται σε μια επίθεση Man In the Middle (MIM) φαίνεται στην Εικόνα 23. Κατά τη διάρκεια αυτής της επίθεσης, ο εισβολέας αποκτά τον έλεγχο ευαίσθητων δεδομένων τροποποιώντας την επικοινωνιακή ζεύξη ανάμεσα σε δύο μέρη, ενώ οι τελικοί χρήστες δεν αντιλαμβάνονται την υποκλοπή (Rani, 2015). Η απώλεια ακεραιότητας (Επίπεδο 1 Εικόνα 20) επιτυγχάνεται με χειρισμό της ροής επικοινωνίας μεταξύ του πελάτη και του διακομιστή δημιουργώντας επιπτώσεις στον κυβερνοχώρο. Τα κλαδιά του δέντρου αντιπροσωπεύουν μεθόδους με τις οποίες οι εισβολείς μπορούν να επιτύχουν το στόχο τους. Τα βέλη στο δέντρο επίθεσης

υποδεικνύουν την ροή της κάθε επίθεσης (Yousef et al., 2018), ενώ η κρυπτογράφηση προσφέρει κάποιο επίπεδο προστασίας (Nichols et al., 2018).



Εικόνα 20. Δενδροδιάγραμμα απειλών (Yousef et al., 2018)

Ωστόσο, συμβιβασμοί συμβαίνουν λόγω των απαιτήσεων αποστολής. Η κρυπτογράφηση μπορεί να υπερφορτώσει συνδέσμους δεδομένων, να καταλάβει πολύτιμο εύρος ζώνης και να προκαλέσει ανεπιθύμητα χαρακτηριστικά πτήσης και ελέγχου, εάν συνδέονται δεδομένα σε πραγματικό χρόνο και απαιτείται έλεγχος για την αποστολή. Η μη χρήση κρυπτογράφησης είναι ένας συμβιβασμός όπως είπε ένας αξιωματούχος του Πενταγώνου, ότι πολλές από τις ροές UAV πρέπει να αποστέλλονται ζωντανά σε πολλά άτομα ταυτόχρονα και βρέθηκε ότι η κρυπτογράφηση επιβραδύνει τον σύνδεσμο σε πραγματικό χρόνο. Επομένως, η κρυπτογράφηση αφαιρέθηκε από πολλές ροές. Η αφαίρεση αυτής όμως επέτρεψε σε τρίτους με τα σωστά εργαλεία να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε αυτές τις επιχειρήσεις (Mount & Quijano, 2009). Δεν υπάρχει μια τέλεια λύση στα ζητήματα ασφαλείας που εμπλέκονται στις επιχειρήσεις UAV, παρά μόνο ένας βαθμός κινδύνου που πρέπει να μετριαστεί (Nichols R. K., 2002

4.4 Είδη λογικών επιθέσεων (παρεμβολών)

Προκειμένου να εξασφαλίσουμε τον ύψιστο βαθμό ασφάλειας πληροφοριών χρειάζεται να βελτιώνεται συνεχώς η μη προσβασιμότητα των δεδομένων, όπως ακριβώς γίνεται για ένα Data-Link. Ενδεικτικά παρατίθενται ορισμένες παρεμβολές.

1. Maldrone, όπου το κακόβουλο λογισμικό βρίσκει πρόσβαση σε κρίσιμες περιοχές του λειτουργικού συστήματος μέσω ελαττωμάτων ασφαλείας στο Data-Link.
2. Πλαστογραφία του GPS είναι μια απειλή που ουσιαστικά μπορεί να αλλάξει ή να καθυστερήσει τις εντολές UAV μέσω GPS και αναλόγως μπορεί να προκαλέσει συγκρούσεις, λανθασμένη καθοδήγηση και θεωρητικά εικονική πειρατεία UAV με την οποία μη στρατιωτικό UAV μπορεί να μετατραπεί σε φορέα επίθεσης εναντίον στρατιωτικών UAV ακόμη και αν το στρατιωτικό GPS προστατεύεται.
3. Zigbee και Killerbee που ουσιαστικά είναι εργαλεία διείσδυσης τα οποία όταν είναι επιτυχημένα μπορεί να προκαλέσουν σοβαρή απειλή λόγω άρνησης υπηρεσίας (Rodday, 2015). Η τεχνολογία Zigbee δημιουργήθηκε με σκοπό την εξυπηρέτηση των ασύρματων προσωπικών δικτύων και στηρίζεται στο πρότυπο IEEE 802.15.4. Λειτουργεί στο φάσμα ISM των 2.4 GHz, ενώ η εμβέλεια μετάδοσης φτάνει ως τα 100 μέτρα και η μέγιστη ταχύτητα 250 Kbps. Το μεγαλύτερο προσόν της εν λόγω της τεχνολογίας αποτελεί η εξαιρετικά χαμηλή κατανάλωση ισχύος που απαιτείται σε πληθώρα σύγχρονων εφαρμογών ενώ μπορεί να δημιουργήσει ευέλικτα και επεκτάσιμα δίκτυα καθώς και να ενσωματώσει νοημοσύνη με στόχο να δημιουργηθούν δίκτυα εισβολής (Στεφανίδης, 2016).

Εικόνα 21. Συσκευή κρυπτογράφησης Kgv-72 Type-1 (Harris Corporation. 2009)

Η κρυπτογράφηση δεδομένων είναι ένα ζωτικό εργαλείο για τη δημιουργία ενός ασφαλούς συνδέσμου δεδομένων. Όπως και στα ενσύρματα δίκτυα υπολογιστών, το ασύρματο UAV χρησιμοποιεί CPU και λειτουργικά συστήματα για την εκτέλεση λειτουργιών που περιλαμβάνουν τεράστιες ποσότητες δεδομένων τα οποία πρέπει να υποβληθούν σε άμεση επεξεργασία και μετάδοση εσωτερικά και εξωτερικά.

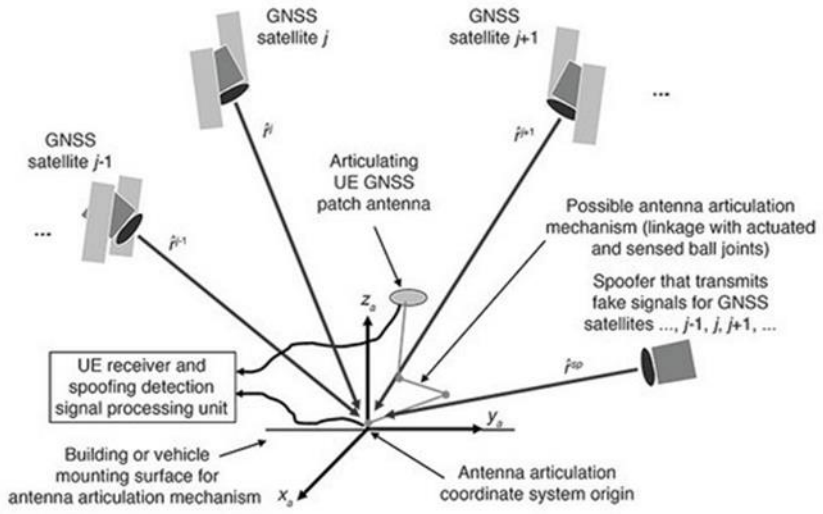
Οποιοδήποτε και αν είναι το πρωτόκολλο ή η τεχνολογία Data-Link δεν πρέπει μόνο να αντιμετωπίζουν τις απειλές που είναι γνωστές σήμερα, αλλά να προσαρμόζονται σε νέες καινούργιες απειλές.

4.5 Αποφυγή παρεμβολής από εχθρό

Ένα ξεχωριστό χαρακτηριστικό του Data-Link –αλλά σε άμεση συσχέτιση- είναι η αποφυγή εξαπάτησης από έναν αντίπαλο. Η πλαστογράφηση μιας φαινομενικά αυθεντικής εντολής ή Σήματος GPS μπορεί να προκαλέσει ανεξέλεγκτη ή ακόμα και συντριβή του UAV. Πρόκειται για πρόβλημα στο ανέβασμα δεδομένων (uplink) μεταξύ βάσης και UAV. Αυτή θεωρείται η επικρατέστερη μέθοδος με την οποία πιστεύεται ότι το Ιράν έχει συλλάβει το αμερικάνικο RQ-170 drone το Δεκέμβριο του 2011, που περιγράψαμε στην περίπτωση 2.

Επί του παρόντος υπάρχουν πολλές μέθοδοι για να επιτευχθεί ένα αποδεκτό επίπεδο αντίστασης σε αυτήν τη μορφή επίθεσης (Nichols et al., 2018). Πολλές μέθοδοι που βοηθούν στην προστασία του Data-Link από άλλες απειλές ασφαλείας παρέχουν επίσης προστασία κατά των επιθέσεων εξαπάτησης. Αυτές περιλαμβάνουν, μετάδοση δεδομένων μέσω Data-Link διευρυμένου φάσματος (Spread Spectrum) χρησιμοποιώντας ασφαλείς κωδικούς ελέγχου ταυτότητας. Αυτοί οι κωδικοί μπορούν να έχουν τη μορφή λογισμικού ενσωματωμένου στη μετάδοση σταθμού εδάφους του UAV. Τόσο ο σταθμός UAV όσο και ο σταθμός εδάφους έχουν λογισμικό κωδικοποίησης και αποκωδικοποίησης για τον έλεγχο της ταυτότητας εντολών χωρίς άμεση τροποποίηση στο uplink. (Fahlstrom, 2012).

Μια ομάδα του πανεπιστημίου Cornell (Nichols et al.2019) ανέπτυξε ένα σύστημα ανίχνευσης πλαστογράφησης GPS, η αρχιτεκτονική του οποίου φαίνεται στην εικόνα 22. Όπως φαίνεται, τρεις δορυφόροι του παγκόσμιου δορυφορικού συστήματος πλοήγησης (GNSS) των οποίων τα σήματα θα ήταν στη μη πλαστογραφημένη θέση: δορυφόροι j-1, j και j + 1. Δείχνει επίσης την πιθανή τοποθεσία ενός πλαστογράφου (spoofer) που θα μπορούσε να στείλει ψευδή σήματα από αυτούς τους δορυφόρους. Ο πλαστογράφος διαθέτει μία κεραία μετάδοσης και οι δορυφόροι j-1, j και j + 1 είναι ορατοί από την κεραία του δέκτη, αλλά ο πλαστογράφος θα μπορούσε να εισβάλει στο βρόχο παρακολούθησης του δέκτη για αυτά τα σήματα, έτσι ώστε μόνο οι ψευδείς πλαστογραφημένες εκδόσεις αυτών των σημάτων να παρακολουθούνται από τον δέκτη (Psiaki et al., 2013).



Spoofing detection antenna articulation system geometry relative to base mount, GNSS satellites, and potential spoofer.

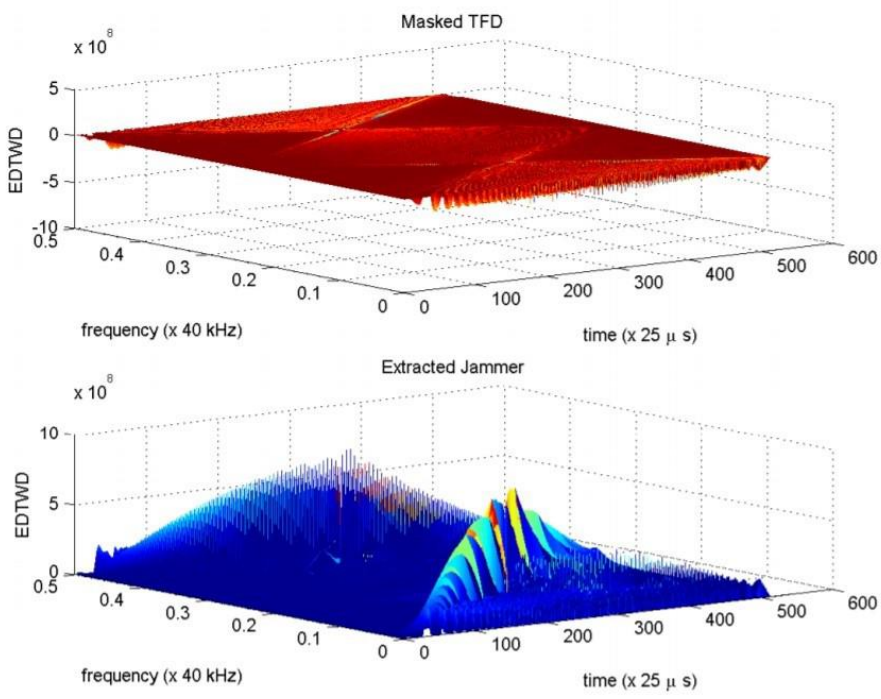
Εικόνα 22. Εξαπάτηση του πλαστογράφου (spoofer) (Kakar, 2017)

Γενικώς οι κίνδυνοι για το Data-Link είναι καθυστέρηση στην αποστολή των δεδομένων, περιορισμένο bandwidth, εξαπάτηση. Όταν το Data-Link εξασφαλίζει ασφαλή δεδομένα υψηλής ταχύτητας επιτρέπει στα ηλεκτρονικά συστήματα να αλληλεπιδρούν απρόσκοπτα με το μηχανικό σύστημα, το οποίο με τη σειρά του μπορεί να παρακολουθεί την απόδοση του ενώ ταυτόχρονα να είναι ευέλικτο σε επιθέσεις. Έτσι διασφαλίζεται η απρόσκοπτη λήψη δεδομένων των αισθητήρων από το downlink. Έτσι, μια άλλη μέθοδος είναι η παρεμβολή των σημάτων, είτε περιέχουν εντολές είτε όχι (jamming), οι οποίες μεταδίδονται από το σταθμό εδάφους. Η παρεμβολή είναι ένα αντίμετρο που χρησιμοποιείται για την αναστολή της ικανότητας του UAV να επικοινωνήσει επιτυχώς με τον χειριστή της αφού προηγουμένως του κατευθύνουν ισχυρή ηλεκτρομαγνητική ακτινοβολία, η οποία λειτουργεί ως θόρυβος στο Data-Link, προκειμένου να μπλοκάρει η επικοινωνία και η μεταφορά δεδομένων στο downlink. Η εμπλοκή της ροής δεδομένων GNSS μεταξύ του UAV και του πιλότου προσβάλει την ικανότητα του UAV για τη σύλληψη εικόνας και ήχου. Χωρίς την ικανότητα να οδηγεί τον εαυτό του ή να οδηγείται από έναν πιλότο που χρησιμοποιεί δεδομένα GNSS, αυξάνει εκθετικά τον κίνδυνο συντριβής, αποτυχίας αποστολής και απώλειας ζωής.

Η παρεμβολή (jamming) για τα UAV είναι μια επίθεση παρόμοια με την επίθεση ωμής βίας σε ένα δίκτυο, έτσι αντί να δημιουργεί τυχαία τεράστιο αριθμό κωδικών πρόσβασης, η εμπλοκή προορίζεται να κατακλύσει με θόρυβο το Data-Link. Η μέθοδος αυτή χρησιμοποιήθηκε κατά κόρον από τα Ρωσικά στρατεύματα στον πόλεμο της Κριμαίας του 2014.

Υπάρχουν διάφορες μέθοδοι αντιμετώπισης της παρεμβολής (Nichols et al., 2018):

- Το διευρυμένο φάσμα (spread spectrum) είναι ένα μέσο μετάδοσης στο οποίο το σήμα καταλαμβάνει ένα bandwidth που υπερβαίνει το ελάχιστο απαραίτητο για την αποστολή των πληροφοριών. Η εξάπλωση της ζώνης επιτυγχάνεται μέσω ενός κώδικα που είναι ανεξάρτητος από τα δεδομένα, ενώ η συγχρονισμένη λήψη – η οποία απαιτεί κωδικό από τον δέκτη- χρησιμοποιείται για τη διάδοση και την επακόλουθη ανάκτηση δεδομένων (Pickholtz et al., 1982)
- Προσαρμοστικό φιλτραρισμα (Adaptive Filtering)
- Φιλτράρισμα χρόνου-συχνότητας (Time – Frequency Domain Filtering)
- Προσαρμοστικές κεραίες (Adaptive Antennas)
- Γραμμικές Αναπαραστάσεις Σημάτων (Bilinear Signal Representations) αναγνωρίζουν τα σήματα παρεμβολής, τα διαχωρίζει και επανασυνθέτει τα νόμιμα σήματα του Data-Link. (Kandangath, 2003) (Collins, 2013). See Figure 13-10 and Figure 13-11 for BSR Representations.



Time-Frequency representation for the masked signal and the extracted jammer. The jammer can be extracted at different threshold levels which depend on the value of α. In this example $\alpha = 3.0$.

Εικόνα 23. Γραμμικές Αναπαραστάσεις Σημάτων (Bilinear Signal Representations (Kandangath, 2003).

Οι παρεμβολές είναι σημαντικές για την παρούσα εργασία επειδή επηρεάζουν κυρίως το uplink, γιατί τυχόν προ-προγραμματισμένες οδηγίες πτήσης μπορούν να οδηγήσουν σε μια επιτυχή αποστολή όταν η παρεμβολή προσβάλει με επιτυχία σήμα από το σταθμό εδάφους προς το UAV. Ωστόσο, εάν μπλοκαριστεί το downlink και διαταραχθεί η αποστολή εικόνων και βίντεο από το UAV προς τον χειριστή, θα

εξαλειφθεί η ευελιξία του ελεγκτή να κάνει προσαρμογές ή αλλαγές στην αποστολή (Fahlstrom, 2012).

4.6 Ταξινόμηση επιθέσεων UAV

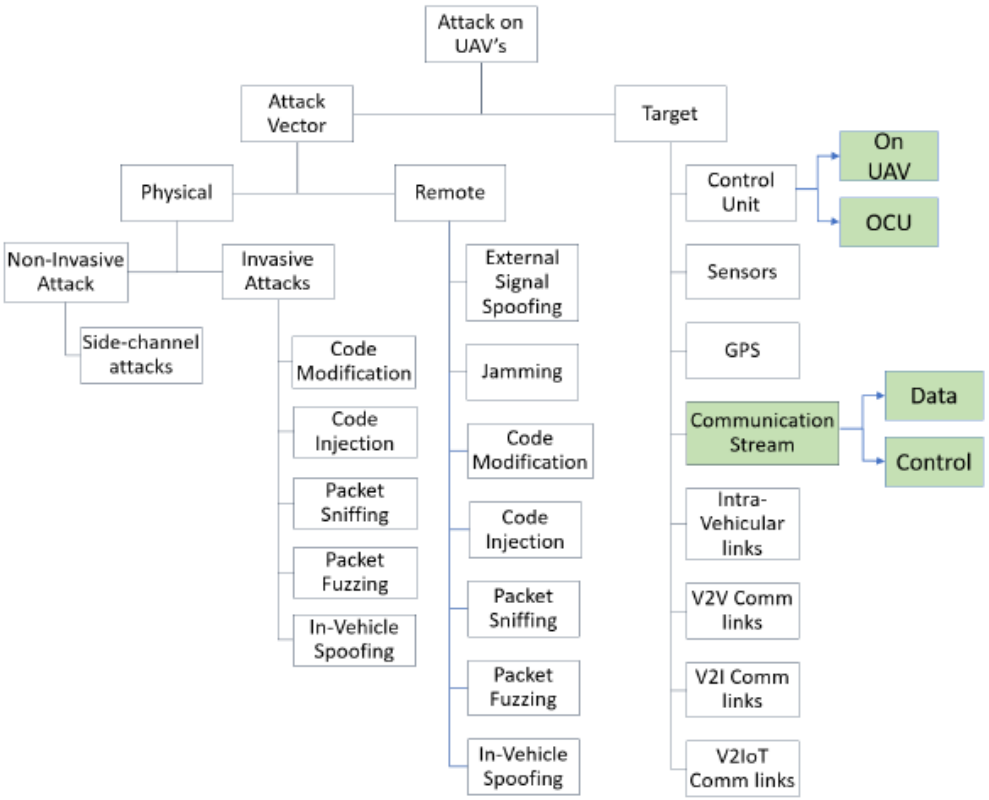
Οι Krishna και Murphy (2017), σε 29 επιστημονικά άρθρα και 11 δημοσιεύματα του τύπου συγκεντρώνουν τη συχνότητα των κινδύνων που προσβάλλουν τα (μεγαλύτερα κυρίως) UAV και τους οργανώνουν σε ταξινομίες.

Η κυρίαρχη είναι η ταξινομία επίθεσης αυτόνομου οχήματος. Στην Εικόνα 24 φαίνεται το σύστημα ενός μικρού εμπορικού drone, το οποίο περιλαμβάνει OCU / GCS, UAV, GPS και τις επικοινωνίες. Το OCU / GCS είναι ένα κέντρο ελέγχου που επιτρέπει τον έλεγχο από τον χειριστή. Η επικοινωνία δεδομένων (που προέρχονται από τους αισθητήρες και για πλοήγηση του drone) χρησιμοποιείται για την αποστολή δεδομένα αισθητήρα, όπως ροή βίντεο, από UAV έως OCU. Τέλος, το UAV επικοινωνεί με δορυφόρο GPS για τριγωνισμό της θέσης του.

Εικόνα 24. Σχήμα ενός μικρού εμπορικού drone με OCU / GCS, UAV, GPS και τις επικοινωνίες Krishna & Murphy, 2017

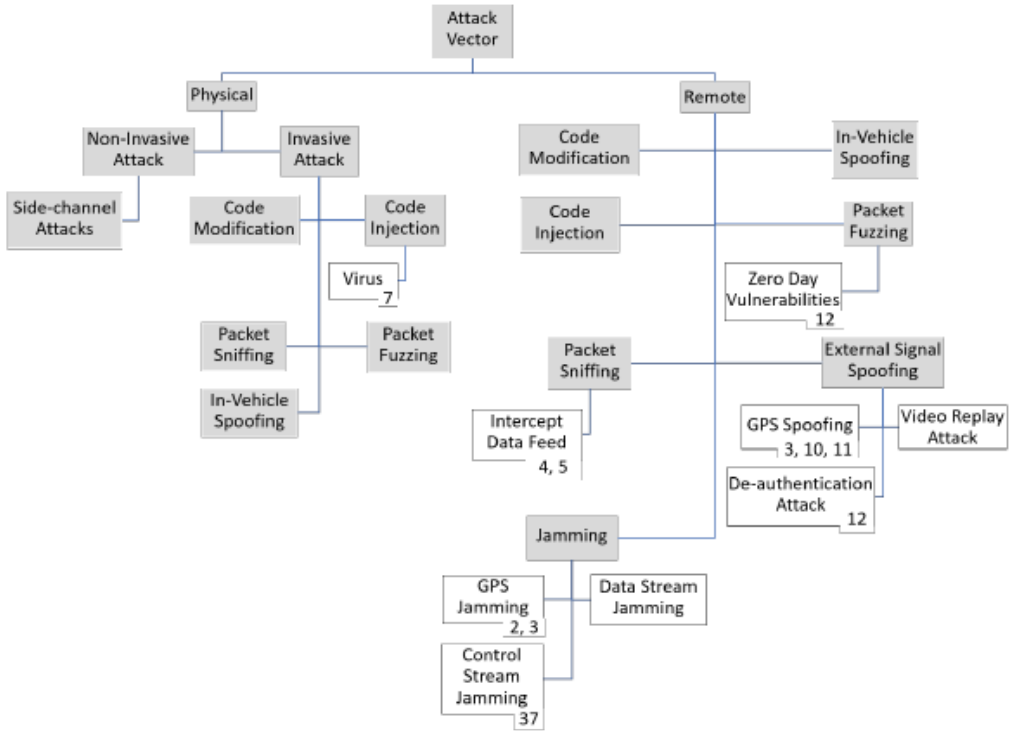
Οι Thing και Wu (2016; Krishna & Murphy, 2017) παρουσίασαν την ταξινομίση επιθέσεων (εικόνα 25) το οποίο παραθέτει όλες τις πιθανές επιθέσεις σε ένα αυτόνομο όχημα, με έμφαση στα αυτοκίνητα χωρίς οδηγό, το οποίο επεκτάθηκε και για τα UAV. Η αρχική ταξινόμηση αποτελείται από πέντε κατηγορίες: τον εισβολέα (attacker), τον φορέα της επίθεσης (attack vector), τον στόχο (target), το κίνητρο (motive) και τις

πιθανές συνέπειες (potential consequences). Η επέκταση τροποποιεί ή προσθέτει υποκατηγορίες στον στόχο, ενώ ο εισβολέας, το κίνητρο και οι πιθανές συνέπειες δεν εμφανίζονται επειδή είναι αμετάβλητα. Η υποκατηγορία ECU (ηλεκτρονική μονάδα ελέγχου) στην ταξινόμηση επίθεσης αυτόνομου οχήματος έχει αντικατασταθεί με την υποκατηγορία μονάδας ελέγχου (control unit), η οποία χωρίζεται περαιτέρω.

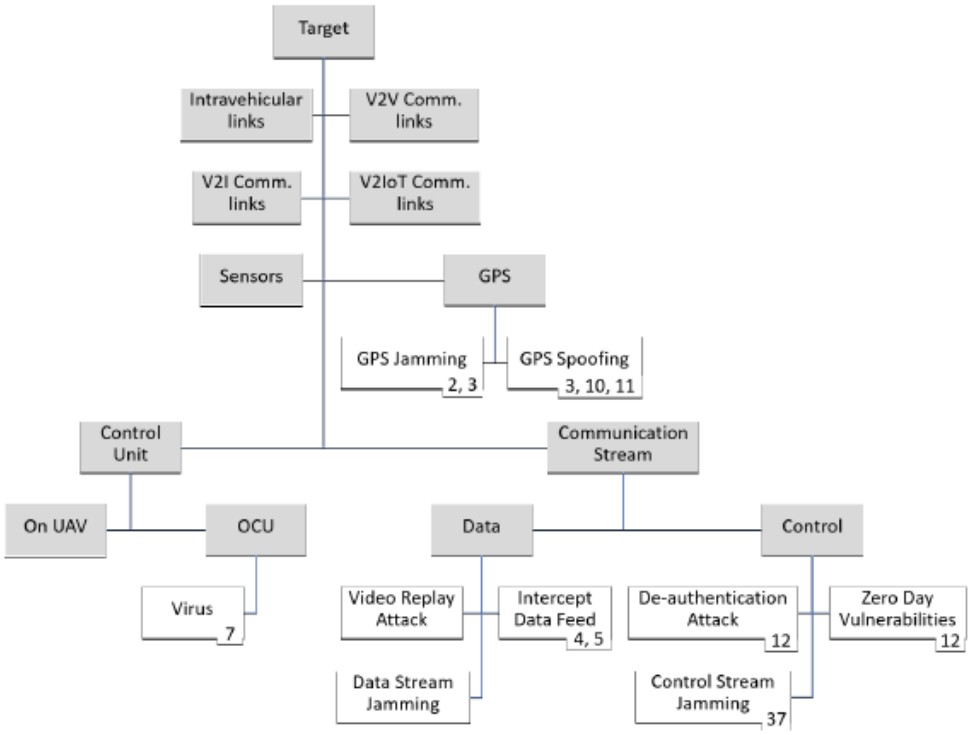


Εικόνα 25.Ταξινομία επίθεσης UAV (Krishna & Murphy, 2017)

Στο προϋπάρχον σχήμα των αυτοκινήτων οι Krishna & Murphy (2017) προσέθεσαν την υποκατηγορία της ροής επικοινωνίας (communication stream), η οποία υποδιαιρείται περαιτέρω στα δεδομένα (data) και τον έλεγχο (control). Πρωταρχικός σκοπός ενός UAV με επίγεια OCU είναι να παρέχει δεδομένα σε πραγματικό χρόνο στους χειριστές του, πράγμα διαφορετικό από ένα αυτοκίνητο χωρίς οδηγό του οποίου η σκοπιμότητα είναι κατά κύριο λόγο τοπική, δηλαδή να παρέχει ενημερώσεις ή επικοινωνία με άλλα αυτοκίνητα ή επόπτες. Τα δεδομένα και οι ροές ελέγχου επικοινωνίας είναι ξεχωριστοί στόχοι, χρήσιμοι όταν ένας εισβολέας προσπαθήσει να μπλοκάρει τη ροή ελέγχου για να συντρίψει το UAV να ή να παρέμβει στη ροή δεδομένων για να παρακολουθήσει τι βλέπει το UAV και πιθανώς να το αλλοιώσει. Στην εικόνα 26 σε κάθε κατηγορία επίθεσης προστίθεται το περιστατικό (σε λευκό ορθογώνιο).



Εικόνα 26 Ταξινομία με τροποποίηση του φορέα επίθεσης (attack vector) (Krishna & Murphy, 2017)



Εικόνα 27. Ταξινομία ως προς τον στόχο (target) (Krishna & Murphy, 2017)

Μεταξύ των επιθέσεων που μπορούν να πραγματοποιηθούν μέσω απομακρυσμένης πρόσβασης σε UAV ή OCU, η τροποποίηση κώδικα (code modification) και η πλαστογράφηση οχήματος (in-vehicle spoofing) δεν έχουν αναφερθεί, αλλά μπορούν να πραγματοποιηθούν εάν η απομακρυσμένη πρόσβαση δεν είναι ασφαλής. Έχουν, όμως, αναφερθεί ένα περιστατικό για το packet fuzzing (ως zero day vulnerilities) και

δύο περιστατικά για το πακέτο οσμανίχνευσης (packet sniffing). Τα ασύρματα (εξωτερικά) σήματα που χρησιμοποιούνται από το σύστημα μπορεί είτε να πλαστογραφηθούν (spoofing) είτε να μπλοκαριστούν (jamming). Στη βιβλιογραφία αναφέρονται τρεις τύποι επιθέσεων (Humphreys et al., 2008; Lictman et al., 2016, Dey, Pudi, Chattopadhyay & Elovici, 2018) που σχετίζονται με την πλαστογράφηση σήματος – πλαστογράφηση GPS (spoofing), επίθεση από-αυθεντικοποίησης (de-authentication) και επίθεση επανάληψης του βίντεο (video replay attack). Οι τρεις τύποι επιθέσεων που σχετίζονται με την παρεμβολή (jamming) και εντοπίζονται στη βιβλιογραφία είναι παρεμβολή του σήματος GPS (GPS jamming), η παρεμβολή της ροής ελέγχου (control stream jaming) και η παρεμβολή της ροής δεδομένων (data stream jamming). Το διάγραμμα της Εικόνας 27 απεικονίζει τους οκτώ πιθανούς στόχους μιας επίθεσης. Το GPS είναι το πλέον στοχευμένο είτε με πλαστογράφηση είτε με παρεμβολή. Αμέσως μετά στοχοποιείται η ροή της επικοινωνίας με επιθέσεις είτε στη ροή ελέγχου (ως από-αυθεντικοποίηση ταυτότητας ή παρεμβολή ή εκμετάλλευση zero day vulnerabilities), η στόχευση ροής δεδομένων (ως παρεμβολή ροής δεδομένων ή επίθεση αναπαραγωγής βίντεο ή παρεμβολή στη ροή δεδομένων). Επόμενος κοινός στόχος είναι η μονάδα ελέγχου (control unit). Δεν αναφέρθηκαν πραγματικές επιθέσεις άμεσα στους αισθητήρες (όπως η κάμερα που είναι συνδεδεμένη με το UAV), αλλά μια επίθεση σε άσκηση προσομοίωσης που άλλαζε την τροχιά του UAV που εκμεταλλευόταν τις προβλέψεις βάσει των δεδομένων των καμερών του. Η επίθεση στην επανάληψη του βίντεο (Video Replay Attack) μπορεί να πραγματοποιηθεί εάν υπάρξει παρεμβολή στο OCU και ο δράστης αντικαταστήσει τη ροή με ένα εγγεγραμμένο βίντεο ολόκληρο ή μέρος αυτού, μέσω μιας εξωτερικής συσκευής. Παρόλο που δεν αναφέρθηκαν περιστατικά για επίθεση στην αναπαραγωγή βίντεο και την παρεμβολή στη ροή δεδομένων (πίνακας 3), οι δύο αυτές επιθέσεις έχουν δυνητικά μεγάλη επίπτωση. Ειδικά αν το UAV λειτουργεί σε FirstPersonView[1] (για μικρά drones) ή είναι εκτός οπτικού πεδίου (για μεγαλύτερα drones) και ο χειριστής δεν αντιληφθεί την παρεμβολή επειδή το βίντεο θα είναι παραπλανητικό (video replay attack) ή δεν θα εμφανίζεται καθόλου (Jamming), το UAV δεν θα μπορέσει να πλοηγηθεί. Πάντως ως αυτή τη στιγμή δεν έχει μελετηθεί και αξιολογηθεί πλήρως αυτή απειλή από δημοσιευμένα άρθρα. Πιθανώς να αποτελεί ήδη

[1] WiFi First Person View (FPV) channel. Είναι ένα κανάλι επικοινωνίας που βασίζεται σε WiFi επικοινωνία και είναι σχεδιασμένο να βλέπει η κονσόλα ελέγχου σε πραγματικό χρόνο την κάμερα και το δεύτερο να πιλοτάρει το drone. Στην πραγματικότητα κάθε μικρό και μεσαίο UAV είναι μια ιπτάμενη κάμερα.

αντικείμενο έρευνας σε στρατιωτικές εφαρμογές των οποίων τα αποτελέσματα είναι διαβαθμισμένα.

Πίνακας 2 είδη και συχνότητες επιθέσεων

Είδος επίθεσης	**Μεγάλα UAV**		**Μικρά UAV**		**Σύνολο**	
	υπαρκτή	προσομοίωση	υπαρκτή	προσομοίωση	υπαρκτή	προσομοίωση
GPS Spoofing	1	0	0	2	1	2
GPS Jamming	1	0	1	0	2	0
Deauthentication	0	0	0	1	0	1
Zero Day Vulnerabilities	0	0	0	1	0	1
Replay Attack	0	0	0	0	0	0
Intercept Data Feed	2	0	0	0	2	0
Virus	1	0	0	0	1	0
Διάφορες	1	0	0	0	1	0
Σύνολο	6	0	1	4	7	4

5. Κρυπτογράφηση πολυμεσικών δεδομένων σε πραγματικό χρόνο

Τα τελευταία χρόνια, η ακαδημαϊκή κοινότητα και η βιομηχανία έχουν επενδύσει στις εφαρμογές του Ίντερνετ των Πραγμάτων (Internet of Things, IoT), ενώ μια από τις κυριότερες εφαρμογές είναι η επεξεργασία πολυμέσων (multimedia sensing) και κυρίως η λήψη και μετάδοση πολυμέσων από μη επανδρωμένα αεροσκάφη (UAV). Τα μη επανδρωμένα συστήματα μπορούν να μειώσουν σε μεγάλο βαθμό τους λειτουργικούς κινδύνους και να επιτύχουν μεγαλύτερη εξοικονόμηση ενέργειας από τα συστήματα ανίχνευσης των παραδοσιακών αεροσκαφών.

Παρ' όλα αυτά, η ασφάλεια των πληροφοριών ήταν ανέκαθεν το κορυφαίο μέλημα και ειδικά στην παρούσα εποχή των δικτύων, όπου όλες οι εφαρμογές IoT βασίζονται στην τεχνολογία επικοινωνίας δικτύου, με όλα τα συνακόλουθα προβλήματα ασφαλείας. Έτσι το ζήτημα της ασφάλειας γίνεται η κεντρική ανησυχία που ενδέχεται να παρεμποδίσει την ανάπτυξη της IoT τεχνολογίας. Όσον αφορά τη λήψη και μετάδοση βίντεο από UAV, το αεροσκάφος μπορεί εύκολα να αιχμαλωτιστεί καθιστώντας ως ευπαθή τα δεδομένα τους. Αυτός είναι ένας από τους λόγους που είναι προτιμότερο να αποστέλλονται σε πραγματικό χρόνο, διαδικασία, όμως, που απαιτεί πολύπλοκη κρυπτογράφηση. Ταυτόχρονα, όμως, υπάρχουν αντικειμενικοί περιορισμοί ως προς το ενεργειακό κόστος και την υπολογιστική επάρκεια. (Ning και Liu, 2012; Chen et al., 2009; Min, 2014; Xiao et al., 2015)

5.1 Ταξινόμηση αλγορίθμων κρυπτογράφησης βίντεο

Σύμφωνα με τη βιβλιογραφία (Shah & Saxena, 2011; Babatunde, Jimoh, & Abikoye, 2017) οι αλγόριθμοι κρυπτογράφησης πολυμέσων διακρίνονται σε τέσσερις κατηγορίες.

5.1.1 Κρυπτογράφηση όλων των επιπέδων (Fully Layered Encryption).

Σε αυτή την κατηγορία ολόκληρο το περιεχόμενο του βίντεο συμπιέζεται πρώτα και στη συνέχεια κάθε byte κρυπτογραφείται στη ροή του MPEG χρησιμοποιώντας παραδοσιακούς αλγορίθμους όπως οι DES, RSA, IDEA, AES. Επειδή η κρυπτογράφηση πραγματοποιείται μετά τη συμπίεση, δεν έχει αντίκτυπο στην απόδοση της δεύτερης. Οι συγκεκριμένοι αλγόριθμοι επεξεργάζονται ως δεδομένα κειμένου όλα τα bytes της ροής του MPEG, με αποτέλεσμα να παρέχουν ασφάλεια σε ολόκληρο βίντεο, επειδή κάθε byte είναι κρυπτογραφημένο και δεν υπάρχει αλγόριθμος που να σπάει το τριπλό DES ή το AES. Ειδικά το τριπλό DES δυσχεραίνει

τις εφαρμογές που απαιτούν βίντεο σε πραγματικό χρόνο, εξαιτίας του μεγάλου υπολογιστικού κόστους και αργής ταχύτητας.

5.1.2 Κρυπτογράφηση βάσει μετάθεσης (Permutation based Encryption)

Κατά τους Shah και Saxena (2011), η κρυπτογράφηση βάσει μετάθεσης χρησιμοποιεί κυρίως διαφορετικούς αλγόριθμους μετάθεσης προκειμένου να ανακατέψουν ή να κρυπτογραφήσουν τα περιεχόμενα του βίντεο. Δεν είναι απαραίτητο να ανακατευτεί κάθε byte. Ορισμένοι αλγόριθμοι χρησιμοποιούν τη λίστα μεταθέσεων ως μυστικό κλειδί για κρυπτογράφηση επιτυγχάνοντας κυρίως την οπτική υποβάθμιση.

Ο Adam J. Slagell (2004) έχει αποδείξει ότι ο απλός αλγόριθμος βάσει μετάθεσης είναι δυνατόν να παραβιαστεί εύκολα από επίθεση, γιατί ο εισβολέας μπορεί να αντιπαραβάλει το κρυπτογραφημένο μήνυμα με τμήματα του αρχικού μηνύματος και να διαπιστώσει τη μυστική λίστα μετάθεσης, ώστε να το χρησιμοποιήσει σε άλλα τμήματα του κρυπτογραφημένου βίντεο που δεν γνωρίζει το αρχικό μήνυμα. Άλλες τροποποιήσεις της μεθόδου είναι: ζιγκ-ζαγκ, κωδικοποίηση Huffman, η τυχαία μετάθεση βασισμένη στη λογική συμπίεσης και η συσχέτιση διατήρησης μετάθεσης.

5.1.2.1 Ζιγκ-ζαγκ

Η μεθοδολογία του "ζιγκ-ζαγκ" εισήχθη από τον Tang (1996) και το σκεπτικό της είναι να αντιστοιχίσει έναν μπλοκ 8x8 σε ένα διάνυσμα 1x64 ακολουθώντας τεθλασμένη διαδρομή και να χρησιμοποιήσει ως μυστικό κλειδί μια τυχαία λίστα μεταθέσεων. Αυτός ο αλγόριθμος αποτελείται από τρία βήματα: (1) δημιουργία μιας λίστας μετάθεσης με 64 στοιχεία, (2) ολοκλήρωση της διαδικασία διαχωρισμού του μπλοκ και (3) εφαρμογή της λίστας τυχαίων μεταθέσεων στο διαχωρισμένο μπλοκ και συνέχιση με την κωδικοποίηση. Αφού η μέθοδος της απλής λίστας μεταθέσεων και αυτή με τεθλασμένη πορεία έχουν παρόμοια υπολογιστική πολυπλοκότητα δεν προκαλεί καθυστέρηση στη συμπίεση του βίντεο αλλά μειώνει τον ρυθμό συμπίεσης, επειδή η τυχαία μετάθεση παραμορφώνει τις σταθερές στην κατανομή πιθανοτήτων του διακριτού μετασχηματισμού συνημίτονων (Discrete Cosine Transform), με αποτέλεσμα ο πίνακας Huffman να μην είναι ο καλύτερος δυνατός. Και πάλι, όμως, ο αλγόριθμος μετάθεσης ζιγκ-ζαγκ δεν μπορεί να αντέξει την επίθεση όταν είναι γνωστά εκ των προτέρων ορισμένα καρέ του βίντεο και μπορούμε εύκολα να καταλάβουμε το μυστικό κλειδί, συγκρίνοντας το γνωστό απλό κείμενο με το αντίστοιχο κρυπτογραφημένο πλαίσιο.

5.1.2.2 Κωδικοποίηση Huffman

Η μετάθεση κωδικοποίησης του Huffman είναι μια ελαφριά κρυπτογράφηση βίντεο που ενσωματώνει κρυπτογράφηση με συμπίεση του MPEG σε ένα βήμα. Ο πρωταρχικός στόχος αυτής της μεθοδολογίας είναι η εξοικονόμηση χρόνου, γιατί εκτελεί ταυτόχρονα τη συμπίεση και την κρυπτογράφηση, χρησιμοποιώντας ως μυστικό κλειδί τη λίστα κωδικοποίησης του Huffman. Για να μην επηρεαστεί ο ρυθμός συμπίεσης, ο αλγόριθμος περιορίζει τη λίστα μετάθεσης μόνο σε όσες κωδικές λέξεις έχουν το ίδιο μήκος με τον τυπικό κωδικό του Huffman.

5.1.2.3 Τυχαία μετάθεση βασισμένη στη λογική συμπίεση

Ο συγκεκριμένος αλγόριθμος αντί να μετατοπίζεται τυχαία τις σταθερές 8x8 ενός μπλοκ, εφαρμόζει την τυχαία μετάθεση σε ορισμένες ομάδες. Κάθε τέτοια ομάδα περιέχει τις σταθερές που έχουν την ίδια συχνότητα σε κάθε μπλοκ ενός πλαισίου, ανεξάρτητα αν το πλαίσιο είναι το I, P ή B. Δεδομένου ότι κάθε μπλοκ έχει 64 συχνότητες σταθερών (προκειμένου να μπορούν να σχηματιστούν 64 ομάδες μετάθεσης), ο περιγραφόμενος αλγόριθμος εκτελεί τυχαίες μεταθέσεις σε καθεμία από τις ομάδες για κρυπτογράφηση ενός μεμονωμένου καρέ του βίντεο. Μετά την τυχαία μετάθεση, τα κρυπτογραφημένα δεδομένα βίντεο συμπιέζονται από ένα σύνηθες RLE. Πρόκειται για έναν επιλεκτικό αλγόριθμο, αφού μόνο ένα μικρός αριθμός ομάδων μετάθεσης μπορεί να κρυπτογραφηθεί βάσει των απαιτήσεων εμπιστευτικότητας. Είναι αξιόπιστο κατά των επιθέσεων ωμής βίας επειδή διαθέτει ένα πολύ μεγάλο εύρος κλειδιών.

5.1.2.4 Συσχέτιση διατήρησης μετάθεσης

Οι περισσότεροι αλγόριθμοι κρυπτογράφησης αποσκοπούν στο να τυχαιοποιήσουν τα δεδομένα προέλευσης, γι' αυτό και δεν μπορούν να εφαρμοστούν αποτελεσματικά πριν από το στάδιο συμπίεσης, αντίθετα με τη συσχέτιση διατήρησης μετάθεσης. Δεν υπάρχει μυστικό κλειδί βάσει του οποίου να γίνει η μετάθεση. Η μέθοδος βασίζεται στην ταξινόμηση της μετάθεσης του προηγούμενου καρέ, με αποτέλεσμα ένα κλειδί να εξαρτάται άμεσα από το απλό κείμενο. Στην περίπτωση επίθεση του απλού κειμένου, ο αντίπαλος μπορεί να υπολογίσει την ταξινόμηση της μετάθεσης για το επιλεγμένο καρέ, αλλά αυτό δεν θα παρέχει πληροφορίες σχετικά με την ταξινόμηση για τα άγνωστα καρέ.

5.1.3 Επιλεκτική κρυπτογράφηση (Selective Encryption)

Αυτοί οι αλγόριθμοι κρυπτογραφούν επιλεκτικά bytes σε ορισμένα καρέ του βίντεο, συνεπώς η υπολογιστική πολυπλοκότητα μειώνεται, αφού δεν πρέπει να γίνει σε όλο

το περιεχόμενο, προσπαθώντας ταυτόχρονα να διατηρήσει ένα επίπεδο ασφάλειας. Σε αυτό το πλαίσιο οι Shah και Saxena (2011), έχουν συγκεντρώσει τις ακόλουθες μεθοδολογίες: των Meyer και Gadegast (1995), των Spanos και Maples (1995), των Shi και Bhargava (1998a, 1998b, 1999), των Wu και Kuo (2001), των Wen, Severa, Zeng, Luttrel και Jin (2002), των Bergeron και Lamy-Bergot (2005), Lian, Liu, Ren και Wang (2004).

Meyer και Gadegast (1995).

Αυτή η μέθοδος χρησιμοποιεί παραδοσιακές μεθόδους κρυπτογράφησης RSA ή DES σε λειτουργία CBC για κρυπτογράφηση της ροής βίντεο. Για το σκοπό αυτό εφαρμόζει τέσσερα επίπεδα ασφάλειας. (1) Κρυπτογράφηση όλων των κεφαλίδων ροής (stream headers), (2) Κρυπτογράφηση όλων των κεφαλίδων ροής και όλων των σταθερών DC και συντελεστών AC των μπλοκ. (3) Κρυπτογράφηση των I-frames και των I-blocks σε P και B-frames. (4) Κρυπτογράφηση όλων των ροών bits. Ο αριθμός των I-blocks P ή B-frames μπορεί να είναι της ίδιας τάξης με τον αριθμό των I-blocks στα I-frames, γεγονός που μειώνει σημαντικά την αποτελεσματικότητα του συστήματος επιλεκτικής κρυπτογράφησης. Ο λόγος κρυπτογράφησης μπορεί να διαφέρει ανάλογα με τις παραμέτρους βάσει των οποίων έγινε η κρυπτογράφηση, π.χ. η κρυπτογράφηση μόνο των κεφαλίδων έχει πολύ μικρότερη αναλογία κρυπτογράφησης, ενώ η κρυπτογράφηση όλων των bitstreams έχει αναλογία 100%. Η ταχύτητα αυτής της μεθοδολογίας και πάλι ποικίλλει λόγω του παραδοσιακού αλγόριθμου που χρησιμοποιείται (π.χ. DES ή RSA) και του πλήθους των παραμέτρων που είναι κρυπτογραφημένες. Ανάλογα με αυτά μπορούν να επιτευχθούν διάφορα επίπεδα ασφάλειας. Για παράδειγμα, δεν επαρκεί η κρυπτογράφηση μόνο των κεφαλίδων, γιατί εύκολα μπορούν να ανακτηθούν, όμως η κρυπτογράφηση όλων των ροών bits μπορεί να προσφέρει υψηλή ασφάλεια. Είναι γεγονός πως δεν έχει γίνει λεπτομερής κρυπτοανάλυση αυτής της μεθοδολογίας, γιατί απαιτούνται ειδικός κωδικοποιητής και αποκωδικοποιητής για να διαβαστεί μια μη κρυπτογραφημένη ροή SECMPEG. Μάλιστα, ο προτεινόμενος κωδικοποιητής δεν είναι συμβατός με αρχεία MPEG.

Spanos και Maples. Ο μηχανισμός Αιγίς (1995) κρυπτογραφεί το περιεχόμενο των frames, τις κεφαλίδες ροής βίντεο και τον κώδικα ISO 32 bit του MPEG χρησιμοποιώντας τον παραδοσιακό αλγόριθμο DES σε λειτουργία CBC. Οι ίδιοι οι συγγραφείς, στα πειράματα που διεξήγαγαν, έδειξαν τη σημασία της επιλεκτικής κρυπτογράφησης στις περιπτώσεις μετάδοσης βίντεο με υψηλά επίπεδα ροής bits, προκείμενου να υπάρχει η ελάχιστη δυνατή καθυστέρηση. Οι Agi και Gong (1996)

απέδειξαν ότι αυτός ο αλγόριθμος έχει χαμηλά επίπεδα ασφάλεια λόγω της κρυπτογράφηση μόνο των I-frames. Επίσης, επεσήμαναν ότι είναι παράλογο να κρυπτογραφούν κεφαλίδες ροής αφού αυτές είναι προβλέψιμες. Επίσης, η προκύπτουσα ροή bits δεν είναι συμβατή με αρχεία MPEG.

Οι Shi και Bhargava (1998a), προτείνουν τον αλγόριθμο κρυπτογράφησης βίντεο που χρησιμοποιεί ένα μυστικό κλειδί, για να αλλάξει τυχαία όλες τις σταθερές DCT σε μια ροή MPEG. Είναι γρήγορο, αφού επεμβαίνει σε ένα μικρό μέρος του πρωτότυπου βίντεο, ενώ είναι πιο αποτελεσματικό από τον αλγόριθμο DES, γιατί κρυπτογραφεί επιλεκτικά ένα μικρό αριθμό bits του MPEG. Στην επόμενη εκδοχή του (1998b) ο αλγόριθμος μειώνει την υπολογιστική πολυπλοκότητα, γιατί κρυπτογραφεί διάφορες σταθερές των I-frames και διαφορικές τιμές των διανυσμάτων κίνησης των P-frames. Αυτή η βελτίωση έχει ως αποτέλεσμα η αναπαραγωγή να είναι τυχαία και λιγότερο εμφανής. Όμως και οι δύο εκδόσεις του αλγορίθμου δεν προστατεύουν από επίθεση απλού κειμένου.

Σε συνεργασία με τον Wang, οι Shi και Bhargava (1999) προτείνουν έναν τρίτο αλγόριθμο –τροποποίηση του προηγούμενου- ο οποίος δίνει έμφαση σε κρυπτογράφηση βίντεο σε πραγματικό χρόνο. Ο αλγόριθμος βασίζεται στον προηγούμενο αλλά αυτή τη φορά διαλέγει 64 bits από κάθε block, με αποτέλεσμα να μειώνει την υπολογιστική πολυπλοκότητα αλλά να διατηρεί έναν μεγάλο αριθμό bits. Η διαφορική κωδικοποίηση των σταθερών DC και των διανυσμάτων κίνησης αυξάνει την δυσκολία να σπάει η κρυπτογράφηση. Αν η αρχική υπόθεση για τις σταθερές DC είναι λανθασμένη, γίνεται πολύ δύσκολο να βρεθούν οι επόμενες τιμές σωστά.

Wu και Kuo (2001). Αρχικά οι συγγραφείς επισημαίνουν ότι, αν μειωθεί η απαιτούμενη ενέργεια, δεν σημαίνει ότι θα μειωθεί και ο βαθμός κατανόησης. Αυτό αποδεικνύεται από το ότι επιτυγχάνεται σημασιολογικά καλή ανασυγκρότηση της εικόνας, όταν το DC έχει σταθερή τιμή και ανακτώνται μόνο οι AC συντελεστές. Ακόμη και αν χρησιμοποιηθεί ένα πολύ μικρό κλάσμα των συντελεστών AC δεν καταστρέφεται πλήρως το σημασιολογικό περιεχόμενο της εικόνας. Οι Wu και Kuo υποστήριξαν ότι είναι ακατάλληλοι για επιλεκτική κρυπτογράφηση τόσο οι αλγόριθμοι συμπίεσης που ακολουθούνται από κβαντοποίηση, όσο και οι αλγόριθμοι συμπίεσης που τελειώνουν με έναν κωδικοποιητή εντροπίας. Αντίθετα, προσπαθούσαν να μετατρέψουν τους κωδικοποιητές εντροπίας σε κρυπτογράμματα. Έτσι, προτείνουν δύο σχήματα για τους πιο δημοφιλείς κωδικοποιητές εντροπίας: τους πολλαπλούς πίνακες Huffman (multiple Huffman tables, MHTs) για τον κωδικοποιητή Huffman και ευρετήριο

πολλαπλών καταστάσεων (multiple state index, MSI) για τον QM αριθμητικό κωδικοποιητής. Στην πρώτη περίπτωση, η ροή δεδομένων εισόδου κωδικοποιείται χρησιμοποιώντας πολλούς πίνακες Huffman, ενώ το περιεχόμενο αυτών των πινάκων και η σειρά που χρησιμοποιούνται, διατηρούνται μυστικά ως το κλειδί της αποκρυπτογράφησης. Αντίθετα με την κωδικοποίηση του Huffman, που χρησιμοποιεί ένα προκαθορισμένο δέντρο Huffman, στην περίπτωση του MSI, επιλέγονται τέσσερις αρχικοί δείκτες κατάστασης, οι οποίοι χρησιμοποιούνται με τυχαία και μυστική σειρά και ο κωδικοποιητής QM τους προσαρμόζει δυναμικά, γεγονός που κάνει δύσκολη την αποκωδικοποίηση αν δεν είναι γνωστοί οι αρχικοί δείκτες κατάστασης.

Οι Wen, Severa, Zeng, Luttrel και Jin (2002), προτείνουν μια μέθοδο κρυπτογράφησης βασισμένη σε κώδικες σταθερού μήκους (Fixed Length Code - FLC και Variable Length Code - VLC). Η μέθοδος αυτή επιλέγει FLC και VLC κωδικές λέξεις που αντιστοιχούν σε σημαντικά πεδία πληροφοριών. Τότε εκχωρείται ένα ευρετήριο κωδικού σταθερού μήκους στον κάθε κωδικό του πίνακα VLC και FLC. Στη συνέχεια οι κρυπτογραφημένοι συνδυασμένοι δείκτες αντιστοιχίζονται σε διαφορετικό αλλά υπάρχον VLC. Όμως, η διαδικασία κρυπτογράφησης θέτει σε κίνδυνο την απόδοση της συμπίεσης, γιατί μερικές σύντομες κωδικές λέξεις VLC (που είναι το πιο πιθανό / συχνό) μπορεί να αντικατασταθούν από μεγαλύτερες, γεγονός που έρχεται σε αντίφαση με την ιδέα της εντροπίας. Αυτό είναι ανταγωνιστικό με την ιδέα της κωδικοποίησης εντροπίας. Παρ'όλα αυτά η πρόταση είναι πλήρως συμβατή με τους αλγόριθμους συμπίεσης.

Bergeron και Lamy-Bergot (2005). Προτείνουν έναν αλγόριθμο κρυπτογράφησης για H.264 / AVC. Η χρήση της προτεινόμενης μεθόδου επιτρέπει την εισαγωγή του μηχανισμού κρυπτογράφησης μέσα στον κωδικοποιητή βίντεο, παρέχοντας μια ασφαλή μετάδοση που δεν μεταβάλλει τη διαδικασία μετάδοσης. Τα προς κρυπτογράφηση bits επιλέγονται σύμφωνα με τον ακόλουθο κανόνα: καθεμία από τις κρυπτογραφημένες ρυθμίσεις τους παρέχει μια μη αποσυγχρονισμένη και πλήρως συμβατή ροή bits. Αυτό μπορεί να γίνει με κρυπτογράφηση μόνο τμημάτων του bitstream που δεν έχουν αντίκτυπο στην εξέλιξη της διαδικασίας αποκωδικοποίησης, με αποτέλεσμα το 25% των I-slices και το 10-15% των P-slice να είναι κρυπτογραφημένο. Το κύριο μειονέκτημα αυτού του σχήματος είναι η έλλειψη κρυπτογραφικής ασφάλεια. Πράγματι, η ασφάλεια του κρυπτογραφημένου bitstream δεν εξαρτάται τόσο από την κρυπτογράφηση AES όσο από το μέγεθος των κωδικών λέξεων. Ως εκ τούτου, η διάχυση της κρυπτογράφησης AES μειώνεται στο μέγεθος του απλού κειμένου.

Lian, Liu, Ren και Wang (2004). Αυτό το σχήμα προτείνεται για Advanced Video Coding - AVC. Κατά τη διάρκεια της κωδικοποίηση του AVC, ευαίσθητα δεδομένα όπως τα διανύσματα κίνησης κρυπτογραφούνται μερικώς. Το σχήμα κρυπτογράφησης έχει υψηλή ευαισθησία κλειδιού, που σημαίνει ότι η μικρή διαφορά στο κλειδί προκαλεί μεγάλες διαφορές στο βίντεο κρυπτογράφησης και αυτό κάνει δύσκολη τη στατιστική ή τη διαφορική επίθεση. Είναι δύσκολο να εφαρμοστεί η επίθεση απλού κειμένου που είναι ήδη γνωστό. Σε αυτό το σχήμα κρυπτογράφησης, κάθε τμήμα κρυπτογραφείται με τον έλεγχο ενός δευτερεύοντος κλειδιού των 128 bit, το οποίο ουσιαστικά απαγορεύει στους επιτιθέμενους να σπάσουν το κρυπτοσύστημα. Σύμφωνα με το σχέδιο κρυπτογράφησης που προτείνεται εδώ, και οι πληροφορίες υφής και αυτές της κίνησης είναι κρυπτογραφημένες, γεγονός που καθιστά δύσκολη την αναγνώριση αυτών των πληροφοριών στα καρέ του βίντεο.

5.1.4 Αντιληπτική κρυπτογράφηση (Perceptual Encryption)

Με την κρυπτογράφηση η ποιότητα των ακουστικών / οπτικών δεδομένων υποβαθμίζεται μόνο εν μέρει, δηλαδή τα κρυπτογραφημένα δεδομένα πολυμέσων παραμένουν μερικώς αντιληπτά μετά την κρυπτογράφηση, δηλαδή κάποιος θα μπορούσε να δει το βίντεο σε χαμηλή ανάλυση. Στην περίπτωση των συνδρομητικών υπηρεσιών που η ποιότητα ήχου και εικόνας είναι το ζητούμενο, ο καταναλωτής θα αναγκαζόταν τελικά να αγοράσει το υψηλής ανάλυσης βίντεο (Shah και Saxena, 2011).

Οι Pazarci και Dipcin (2002) πρότειναν ένα αντιληπτικό σχήμα κρυπτογράφησης MPEG-2, το οποίο κρυπτογραφεί το βίντεο στο RGB χρωματικό φάσμα μέσω τεσσάρων μυστικών γραμμικών μετασχηματισμών πριν τη συμπίεση από τον κωδικοποιητή MPEG-2. Η προτεινόμενη λύση είναι ένα διαφανές ανακάτεμα του MPEG-2 που επιτρέπει στους μη εξουσιοδοτημένους χρήστες να έχουν υποβαθμισμένη προβολή του τρέχοντος προγράμματος. Το ανακάτεμα πραγματοποιείται πριν από την κωδικοποίηση MPEG και το αποτέλεσμα είναι ένα MPEG-2 βίντεο, το οποίο έχει κωδικοποιηθεί με μια ελάχιστη αύξηση στο ρυθμό ροής των bits. Το κύριο πλεονέκτημα του συστήματος των Pazarci και Dipcin είναι ότι η κρυπτογράφηση / αποκρυπτογράφηση και η κωδικοποίηση / αποκωδικοποίηση του MPEG είναι δύο διακριτές λειτουργίες, με αποτέλεσμα το μέρος της κρυπτογράφησης μπορεί απλά να προστεθεί σε ένα σύστημα MPEG χωρίς καμία τροποποίηση, αλλά πάντα υπάρχει ο κίνδυνος να μην λειτουργήσει ο αλγόριθμος αντιστάθμισης κίνησης για τα κρυπτογραφημένα βίντεο. Επιπλέον, ο αλγόριθμος δεν είναι αρκετά ασφαλής ενάντια σε επιθέσεις απλού κειμένου που είναι ήδη γνωστό.

Οι Lian, Wang, Sung και Wang (2004) προτείνουν ένα σχήμα για συμπιεσμένα 3D-SPIHT βίντεο, το οποίο υποβαθμίζει το βίντεο σε διαφορετικό βαθμό. Η ισχύς της κρυπτογράφησης μπορεί να προσαρμόζεται σύμφωνα με συγκεκριμένους συντελεστές ποιότητας. Φυσικά και αυτός ο αλγόριθμος δεν είναι ασφαλής απέναντι στην επίθεση απλού κειμένου που είναι ήδη γνωστό.

Οι Wang, Yu και Zheng (2003) πρότειναν ένα σχήμα που λειτουργεί σε DCT συμπίεση. Σε αυτό το σχήμα εισάγονται τρεις νέες παράμετροι k_1, k_2, k_3 για τον προσδιορισμό των τιμών του a_i για το χρωματικό χώρο YCbCr. Οι 16 τιμές από a_0 έως a_{15}, οι δύο παράγοντες ελέγχου, beta και C και οι τρεις παράμετροι k_1, k_2, k_3 χρησιμεύουν ως μυστικές παράμετροι. Παρ'ότι η μείωση του λόγου συμπίεσης των αντισταθμίσεων κίνησης αποτρέπει την κρυπτογράφηση να αλλάξει τη φυσική κατανομή των συντελεστών DCT και έτσι μειώνεται η αποτελεσματικότητα της συμπίεσης του κωδικοποιητή εντροπίας Huffman. Επιπλέον, εάν οι μυστικές παράμετροι ενσωματώνονται σε υψηλής ποιότητας συχνότητα των συντελεστών DCT για μετάδοση, η απόδοση συμπίεσης θα τεθεί σε κίνδυνο. Ο αλγόριθμος δεν είναι ακόμη αρκετά ευαίσθητος στην αναντιστοιχία μυστικών παραμέτρων, γιατί η συνάρτηση της κρυπτογράφησης και η συνάρτηση υπολογισμού a_i διατηρούνται γραμμικά. Επιπλέον, δεν είναι επαρκώς ασφαλής σε επιθέσεις λόγω των περιορισμένων τιμών του a_i, beta, C, k_1, k_2, k_3. Τέλος, το σχήμα είναι μη ασφαλές απέναντι σε επιθέσεις απλού κειμένου, γιατί το a_i μπορεί εύκολα να υπολογιστεί από το προηγούμενο I-frame του απλού βίντεο.

Οι Li, Chen, Cheung, Bharat Bhargava και Kwok-Tung Lo (2007) προτείνουν μια γενικευμένη έκδοση του VEA για ένα αντιληπτικό σχήμα κρυπτογράφησης, το οποίο κρυπτογραφεί επιλεκτικά στοιχεία δεδομένων FLC στη ροή του βίντεο. Προφανώς, η κρυπτογράφηση των FLC στοιχείων είναι ο πιο φυσικός τρόπος να διατηρηθεί το μεγέθος. Προκειμένου να διατηρηθεί η μορφή συμμόρφωσης λαμβάνονται υπόψη μόνο τα τέσσερα τελευταία στοιχεία δεδομένων FLC. Η αποτελεσματικότητα απέναντι σε απειλές απλού κειμένου που είναι γνωστό διασφαλίζεται από διαφορετικά μέτρα, όπως είναι η εφαρμογή μπλοκ κρυπτογράφησης, η επανατροφοδότηση κρυπτογράμματος και η χρήση ροή κρυπτογράφησης με μοναδικό αναγνωριστικό (ID).

5.2 Κριτήρια αξιολόγησης αλγορίθμων κρυπτογράφησης

Προκειμένου να αξιολογήσουμε ποιος αλγόριθμος είναι ο καταλληλότερος για την κρυπτογράφηση πολυμεσικών δεδομένων σε μη επανδρωμένα αεροσκάφη και

drones, αξιολογούμε τους αλγορίθμους βάσει των παρακάτω παραμέτρων (Shah & Saxena, 2011; Babatunde, Jimoh, & Abikoye, 2017):

- Οπτική υποβάθμιση: Αυτό το κριτήριο μετρά την αντιληπτή παραμόρφωση των δεδομένων βίντεο σε σχέση με το απλό βίντεο. Σε ορισμένες εφαρμογές, όπως π.χ. η συνδρομητική τηλεόραση, θα ήταν επιθυμητό, ένας εισβολέας θα κατανοούσε ακόμα το περιεχόμενο, αλλά θα προτιμούσε να πληρώνει την πρόσβαση στο μη κρυπτογραφημένο περιεχόμενο. Ωστόσο, για ευαίσθητα δεδομένα, είναι επιθυμητή η πλήρης απόκρυψη του οπτικού περιεχομένου.
- Αναλογία κρυπτογράφησης (Encryption ratio): Μετρά την αναλογία μεταξύ του μεγέθους του κρυπτογραφημένου μέρους και του συνολικού μεγέθους των δεδομένων. Προκειμένου να μειωθεί η υπολογιστική πολυπλοκότητα, ο λόγος κρυπτογράφησης πρέπει να ελαχιστοποιηθεί.
- Ταχύτητα (Speed): Σε πολλές εφαρμογές πολυμέσων σε πραγματικό χρόνο οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης πρέπει να είναι αρκετά γρήγοροι.
- Φιλικότητα στη συμπίεση (Compression Friendliness): Είναι επιθυμητό ένας αλγόριθμος κρυπτογράφησης να έχει πολύ μικρή επίδραση στην απόδοση συμπίεσης δεδομένων, γιατί οι περισσότεροι αλγόριθμοι εισάγουν πρόσθετα δεδομένα απαραίτητα για την αποκρυπτογράφηση.
- Συμμόρφωση μορφοποίησης (Format Compliance): Η κρυπτογραφημένη ροή των bytes πρέπει να συμμορφώνεται με τον συμπιεστή, ενώ ο αποκωδικοποιητής οφείλει να αποκωδικοποιεί την κρυπτογραφημένη ροή.
- Κρυπτογραφική ασφάλεια (Cryptographic Security): καθορίζει εάν ο αλγόριθμος κρυπτογράφησης είναι ασφαλής σε πάσης φύσεως επίθεση εναντίον του αρχικού κομματιού πληροφορίας-κρυπτογράμματος (Λημνιώτης, 2020). Ειδικά στην περίπτωση πολυμεσικών δεδομένων για drones είναι καίριο να διασφαλίζεται η κρυπτογραφική ασφάλεια.

Πίνακας 3. Σύγκριση των αλγορίθμων (Shah & Saxena, 2011)

Κατηγορία αλγορίθμου	Όνομα αλγορίθμου	Οπτική υποβάθμιση	Αναλογία κρυπτογράφησης	Ταχύτητα	Φιλικότητα συμπίεσης	Συμμόρφωση μορφοποίησης	Κρυπτογραφική ασφάλεια
Κρυπτογράφηση όλων των επιπέδων		Υψηλή	100%	Αργή	✓	✓	?
Κρυπτογράφηση βάσει μετάθεσης	Απλή μετάθεση	Υψηλή	100%	Γρήγορη	×	✓	?
	ζιγκ-ζαγκ	?	100%	Γρήγορη	×	✓	?
	κωδικοποίηση Huffman	?	?	Γρήγορη	×	×	?
	τυχαία μετάθεση βασισμένη στη λογική συμπίεσης	Μεταβλητή	Μεταβλητή	Γρήγορη	?	✓	✓
	συσχέτιση διατήρησης μετάθεσης	?	?	Γρήγορη	✓	✓	✓
Επιλεκτική κρυπτογράφηση	Meyer και Gadegast (1995)	Μεταβλητή	Μεταβλητή	Μεταβλητή	Μεταβλητή	✓	×
	Spanos και Maples (1995)	?	Υψηλή	?	×	✓	×
	Shi και Bhargava (1998a, 1998b)	Υψηλή	?	Γρήγορη	×	✓	✓
	Shi, Wang και Bhargava (1999)	Υψηλή	?	Γρήγορη	×	×	✓
	Wu και Kuo (2001)	Υψηλή	Μεταβλητή	?	×	✓	×
	Wen, Severa, Zeng, Luttrel και Jin (2002)	Υψηλή	<15%	?	?	×	✓
	Bergeron και Lamy-Bergot (2005)	Υψηλή	×	?	×	✓	✓

	Lian, Liu, Ren και Wang (2004)	Υψηλή	?	Υψηλή	✓	?	✓

6. Σχεδιασμός και υλοποίηση αλγορίθμου AES-128 για βίντεο

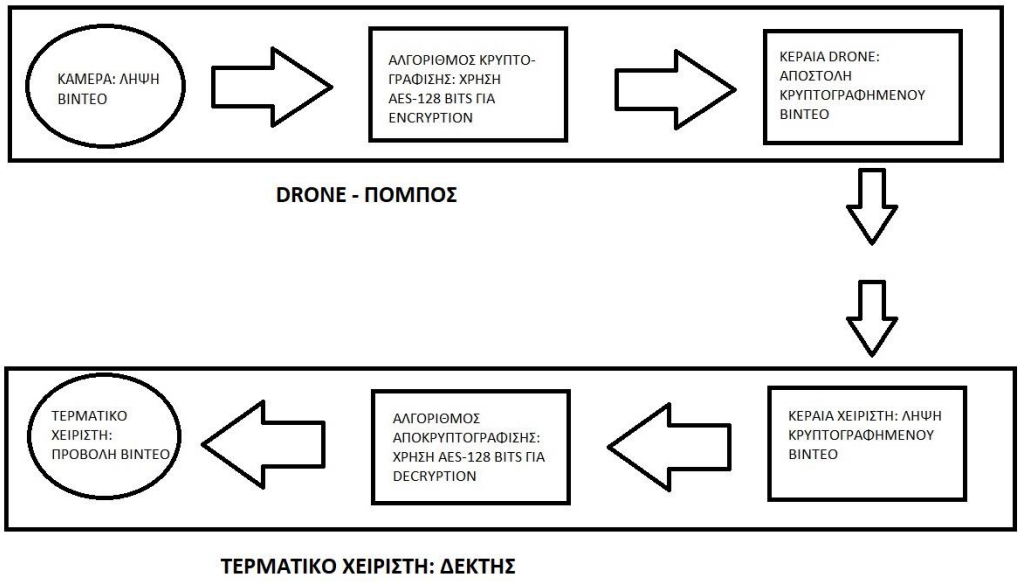
6.1 Διάγραμμα ενεργειών και λόγοι επιλογής AES-128

Αν και τα μη επανδρωμένα ιπτάμενα αεροσκάφη (UAV) βασίζονται στη λήψη βίντεο τόσο για την πλοήγηση εκτός οπτικού πεδίου όσο και για τη λήψη πληροφοριών, η λήψη και αποστολή μεγάλου όγκου δεδομένων σε πραγματικό χρόνο είναι περισσότερο ευάλωτες σε μη επανδρωμένο σύστημα από αυτό του επανδρωμένου συστήματος, ενώ η υπολογιστική ισχύ και οι διαθέσιμοι ενεργειακοί πόροι είναι ιδιαίτερα περιορισμένοι, γεγονός που περιορίζει τη χρήση σύνθετης διαδικασίας κρυπτογράφησης βίντεο. Όμως, πιο σημαντικός στόχος είναι η διασφάλιση της εμπιστευτικότητας των δεδομένων βίντεο ανεξαρτήτως των περιορισμένων πόρων (Xiao, et al., 2015) και επειδή στην παρούσα εργασία, η οποία αφορά σε στρατιωτική χρήση, προέχει η ασφάλεια, επιλέγεται η πλήρης κρυπτογράφηση του βίντεο και η συμπίεση (είτε πριν είτε μετά την κρυπτογράφηση). Σημαντική επίσης είναι η επιλογή του σωστού format βίντεο, ώστε ήδη από την κρυπτογράφηση να παράγονται πολυμεσικά δεδομένα που έχουν το μικρότερο δυνατό μέγεθος και υπολογιστική πολυπλοκότητα και θα αναλύσουμε στην ενότητα αποτελέσματα.

Η συμπίεση είναι απαραίτητη για να τη μείωση του υπολογιστικού κόστους. Οι περισσότεροι ερευνητές που είδαμε στην προηγούμενη ενότητα εξετάζουν διαφορετικά βήματα συμπίεσης βίντεο κατά τη διάρκεια της οποίας γίνεται η κρυπτογράφηση. Αρκετά συστήματα επιλέγουν τη μερική ή επιλεκτική κρυπτογράφηση. Αυτή η κατηγορία αξιοποιεί τα πλεονεκτήματα της βιβλιογραφίας για τη συμπίεση πολυμέσων με ταυτόχρονη χρήση των παραδοσιακών αλγορίθμων κρυπτογράφησης ακριβώς μετά από ή σε ένα συγκεκριμένο βήμα της συμπίεσης του βίντεο. Εκτός από τα μέρη των δεδομένων που έχουν κρυπτογραφηθεί, τα εναπομείναντα δεδομένα μεταδίδονται ως απλό κείμενο, το οποίο μπορεί να υποκλαπεί εύκολα και γρήγορα επιτρέποντας με σχετική δυσκολία τη μερική αναδημιουργία ενός βίντεο.

Για να ισοσταθμίσουμε την όποια καθυστέρηση προκύψει από την πλήρη κρυπτογράφηση, χρησιμοποιούμε τον AES-128. Σε σύγκριση με την κρυπτογράφηση

ροής, η κρυπτογράφηση σε block όπως ο αλγόριθμος AES μπορούν να παρέχουν καλύτερη προστασία με μικρότερα κλειδιά. Τα κλειδιά συνεδρίας (session keys) και τα κλειδιά καναλιού channel keys) είναι δύο μέρη του κλειδιού AES, τα οποία μεταδίδονται και ενημερώνονται ξεχωριστά για να διασφαλιστούν. Στο AES, ο κρυπτογράφος παίρνει ένα μέγεθος μπλοκ απλού κειμένου 128 bits ή 16 bytes. Το μήκος του κλειδιού μπορεί να είναι 16, 24 ή 32 bytes (128, 192 ή 256 bits).



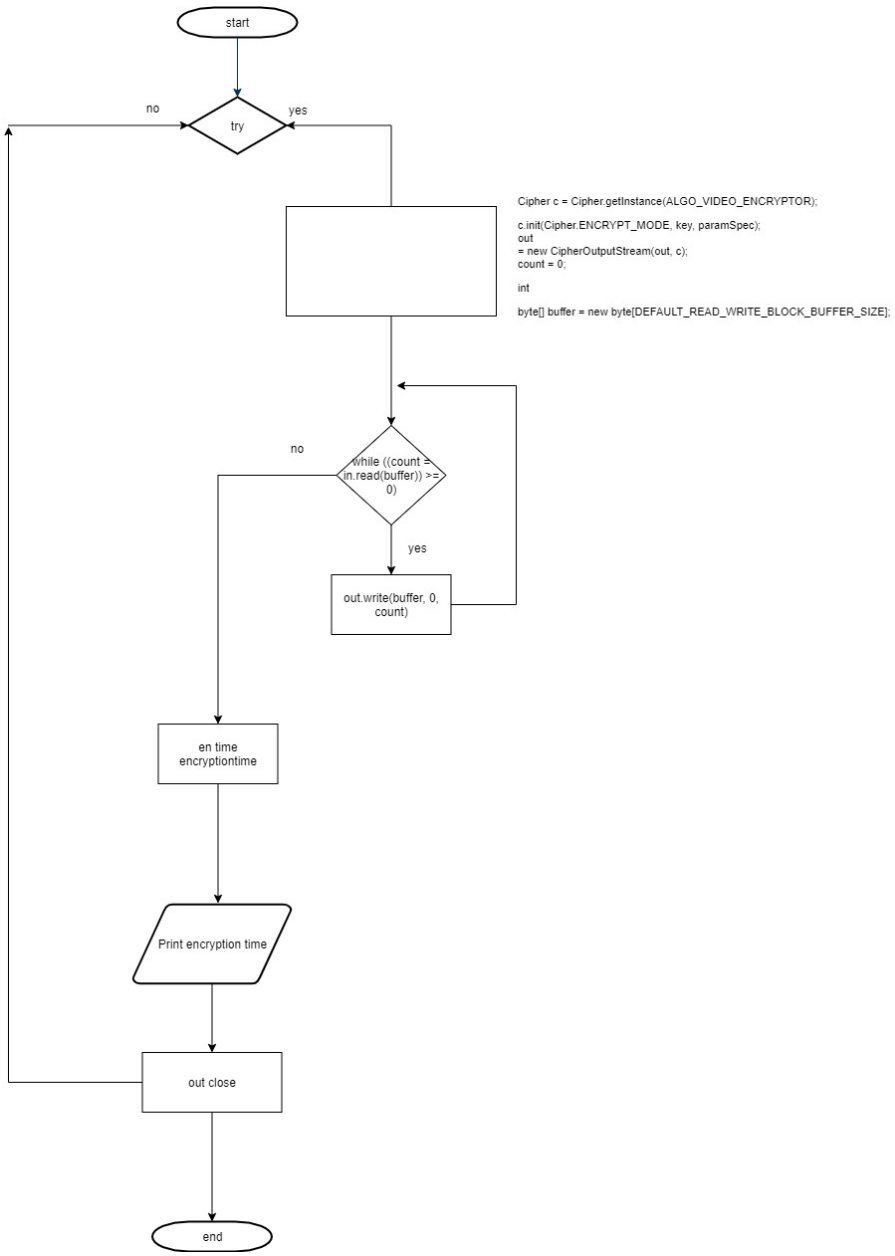
Εικόνα 28. Διάγραμμα ενεργειών

Τέλος, για την υλοποίηση του αλγόριθμου, προτιμήθηκε η JAVA. Παρ' ότι η πλειοψηφία των κατασκευαστών πολιτικών και στρατιωτικών drones τα προγραμματίζουν σε C ή C ++, αλλά ως γνωστό έχουν ευπάθειες. Οι επιτιθέμενοι έχουν χάσει πολλά εμπορικά drones, επειδή είναι προγραμματισμένα με C ++. Μια χαρακτηριστική περίπτωση είναι τα drones της αμερικανικής 3D Robotics, η οποία χρησιμοποιεί πλατφόρμες ανάπτυξης ανοιχτού κώδικα που περιλαμβάνουν C ++ και είναι ευάλωτο σε κυβερνοεπιθέσεις, ενώ αντίθετα τα UAV της DJI υποστηρίζουν μόνο το Android Studio SDK, το οποίο χρησιμοποιεί Java για τις εφαρμογές και δεν είναι τόσο ευάλωτες όσο τα drone που έχουν προγραμματιστεί με C ή C ++ (Mohan, 2016). Βέβαια στην ενότητα 2 επισημάναμε ότι η κυβέρνηση των ΗΠΑ απαγόρευσε τη χρήση των DJI για κενά ασφαλείας, αλλά κυρίως γιατί η ίδια η κινεζική εταιρεία μπορούσε να αντλήσει πληροφορίες και όχι ένας τρίτος εισβολέας. Η καταλληλότητα της Java για τέτοιου είδους εφαρμογές ορίζεται τόσο από την ασφάλεια που προσφέρει σε

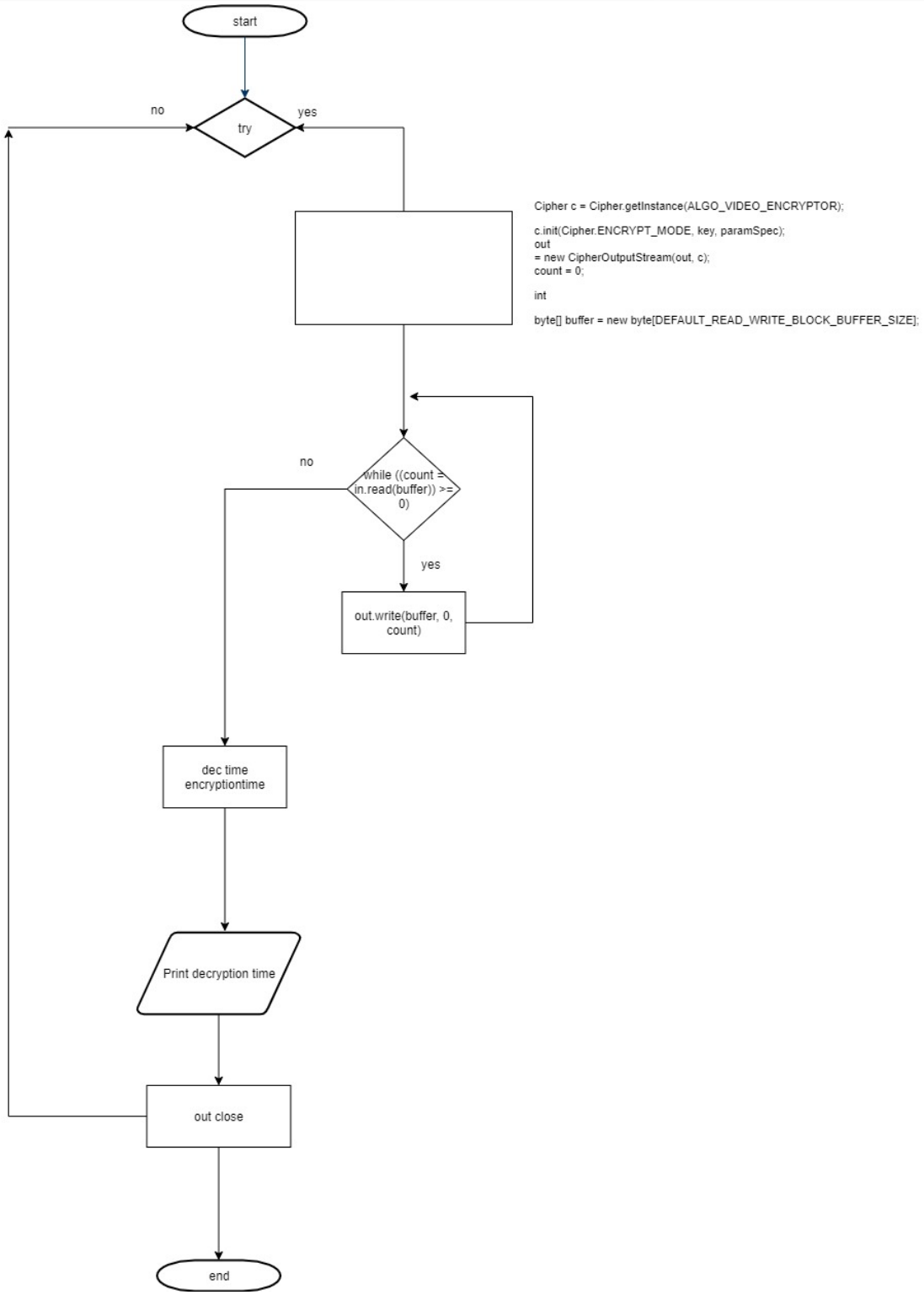
κυβερνοεπιθέσεις, όσο και από τη διάδοση του Android, η οποία επιτρέπει ευρεία χρήση.

6.2 Διαγράμματα ροής αλγορίθμου

Στη συνέχεια παρατίθενται τα διαγράμματα ροής του αλγορίθμου για την κρυπτογράφηση και την αποκρυπτογράφηση. Ο κώδικας βρίσκεται στο παράρτημα.



Εικόνα 29. Διάγραμμα ροής κρυπτογράφησης



Εικόνα 30. Διάγραμμα ροής αποκρυπτογράφησης

6.3 Αποτελέσματα

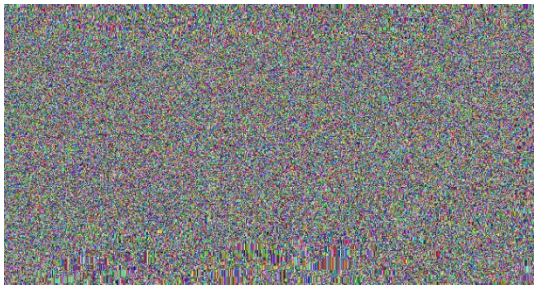
6.3.1 Εικόνα αρχικού βίντεο, κρυπτογραφημένου και ιστογράμματά τους για RGB

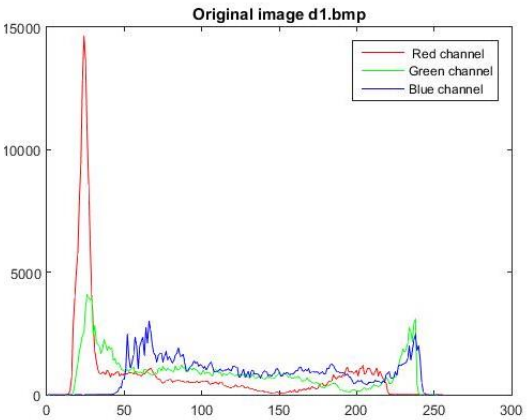
Προκειμένου να δοκιμασθεί ο αλγόριθμος και να ελεγχθεί η αποτελεσματικότητα της κρυπτογράφησης χρησιμοποιήθηκαν δύο βίντεο. Το πρώτο βίντεο είναι τραβηγμένο από drone και εικονίζει έναν παραθαλάσσιο οικισμό, με χρώματα κα εικόνες αντιπροσωπευτικά για τη νησιωτική χώρα, η οποία έχει μεγάλες ανάγκες εναέριας επιτήρησης. Επειδή, όμως, έχει κυρίως μπλε χρώμα προκειμένου να δείξουμε καλύτερα τον αλγόριθμο επιλέξαμε ένα επιπλέον βίντεο στο οποίο εμφανίζονται όλα τα χρώματα (και κυρίως το κόκκινο).

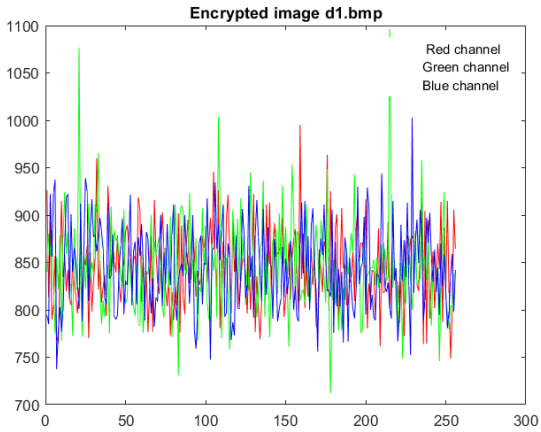
Για ολόκληρα τα βίντεο αρχικά, κρυπτογραφημένα και αποκωδικοποιημένα πρβ. https://drive.google.com/open?id=1e8NwtRhiy_SmdAZtdrxaevAOKM7WQVed

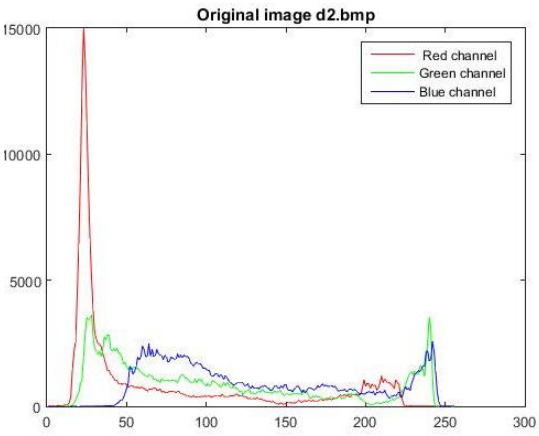
Πιο συγκεκριμένα, στις παρακάτω λήψεις φαίνονται τα ιστογράμματα της αρχικής και κωδικοποιημένης λήψης. Το κρυπτογραφημένο έχει παντού πολύ καλή παραμόρφωση που καθιστά την αναγνώριση της εικόνας αδύνατη. Η θορυβώδης εικόνα είναι εμφανής και στα ιστογράμματα του κρυπτογραφημένου βίντεο για τα τρία βασικά χρώματα (κόκκινο, πράσινο και μπλε RGB) σε αντίθεση με τα ιστογράμματα του αρχικού βίντεο που εμφανίζουν τη σωστή κατανομή των χρωμάτων.

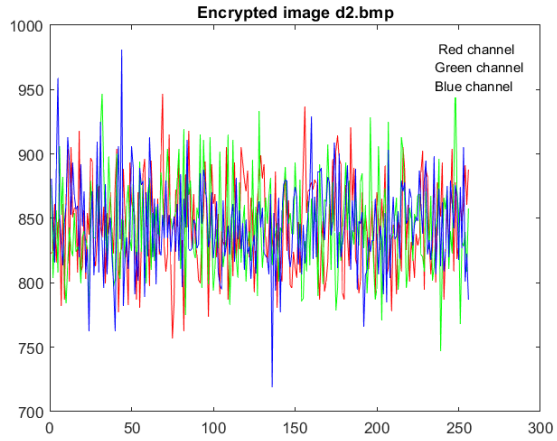
Εικόνες 31. Στιγμιότυπα αρχικού βίντεο, κρυπτογραφημένου και ιστογράμματά τους για το RGB

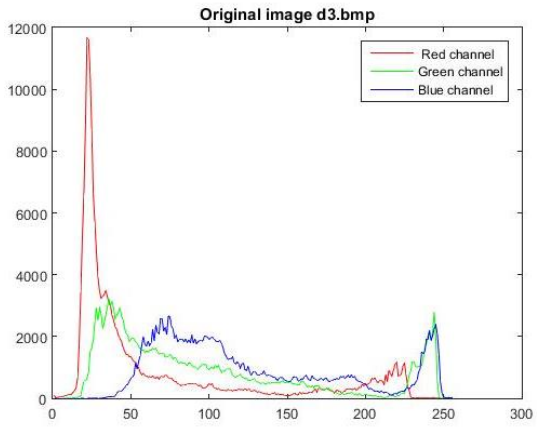


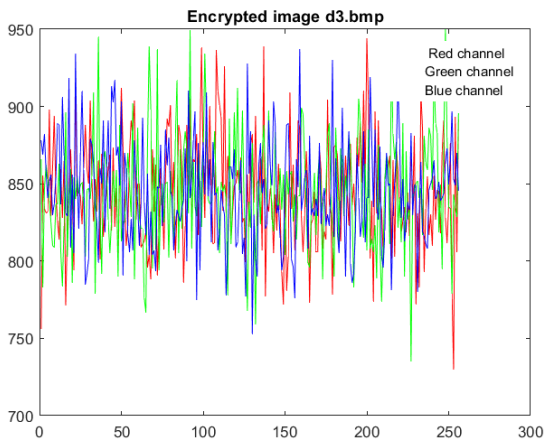


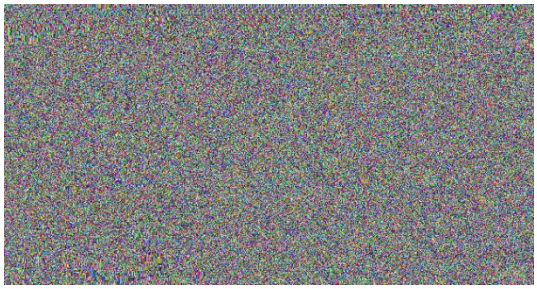


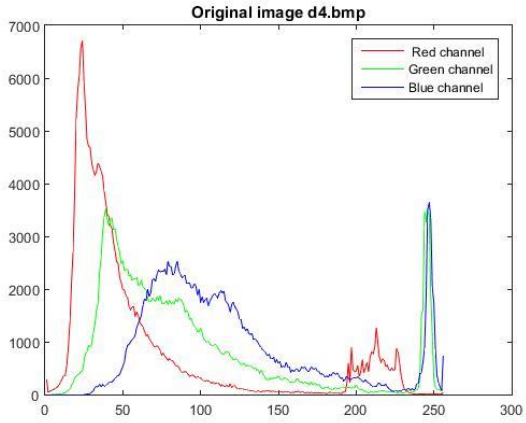

Original image d2.bmp
Red channel
Green channel
Blue channel
15000
10000
5000
0
0
50
100
150
200
250
300

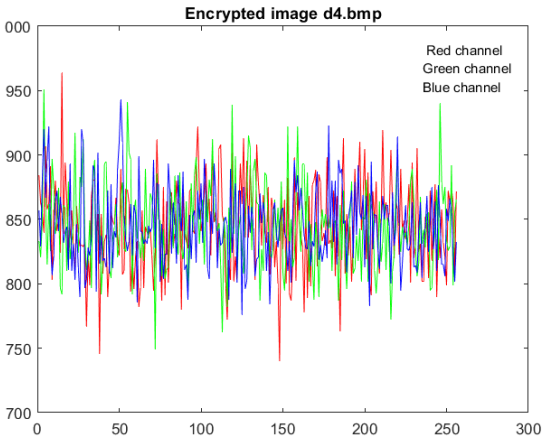

Encrypted image d2.bmp
Red channel
Green channel
Blue channel
1000
950
900
850
800
750
700
0
50
100
150
200
250
300

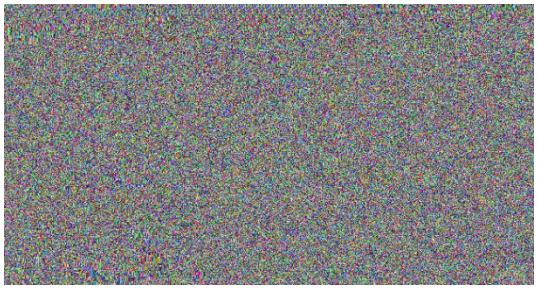

Original image d3.bmp
Red channel
Green channel
Blue channel
12000
10000
8000
6000
4000
2000
0
0
50
100
150
200
250
300

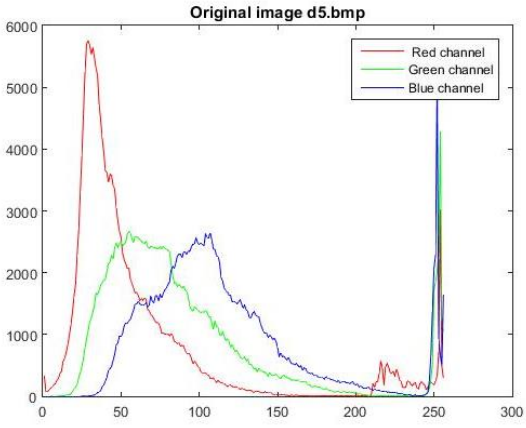

Encrypted image d3.bmp
Red channel
Green channel
Blue channel
950
900
850
800
750
700
0
50
100
150
200
250
300

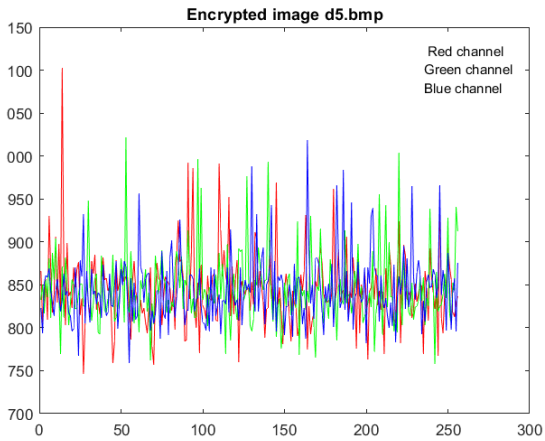


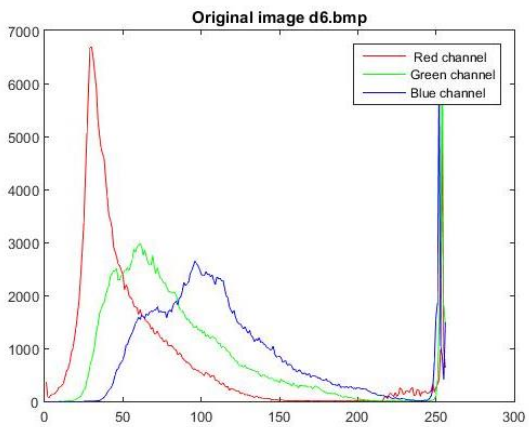

Original image d4.bmp
Red channel
Green channel
Blue channel

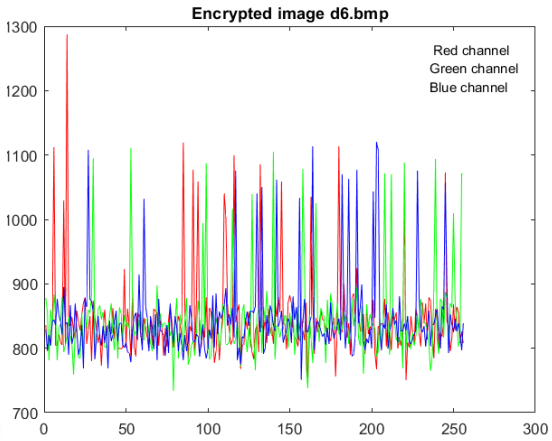

Encrypted image d4.bmp
Red channel
Green channel
Blue channel

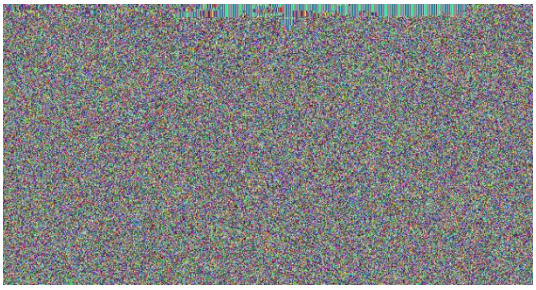


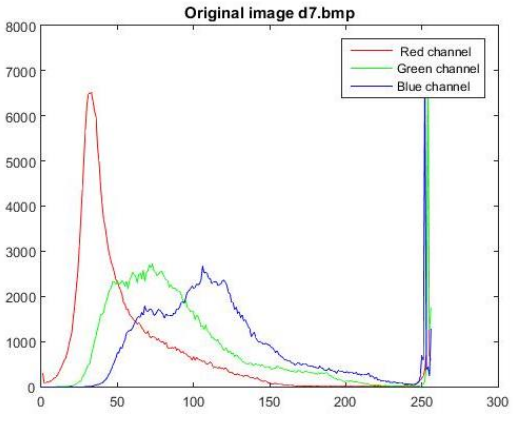

Original image d5.bmp
Red channel
Green channel
Blue channel

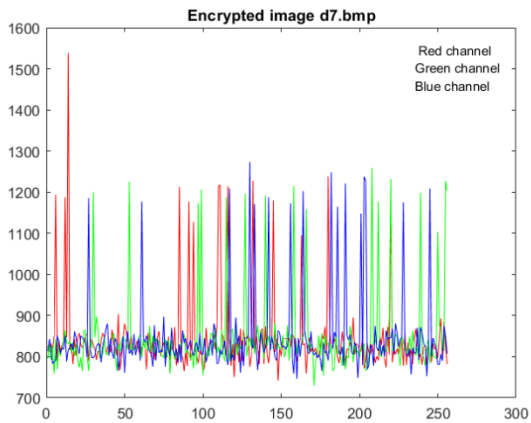

Encrypted image d5.bmp
Red channel
Green channel
Blue channel

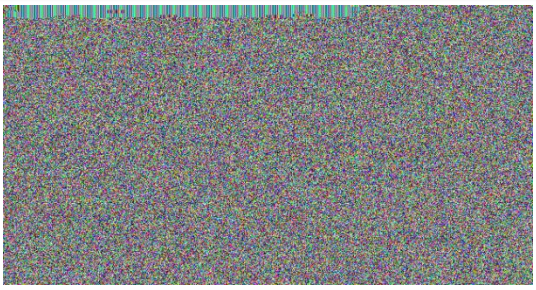

Original image d6.bmp
Red channel
Green channel
Blue channel
0
1000
2000
3000
4000
5000
6000
7000
0
50
100
150
200
250
300

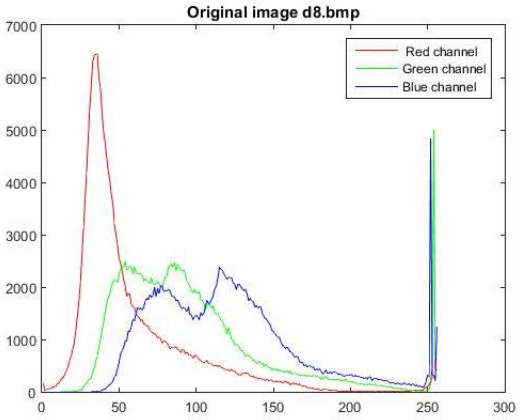

Encrypted image d6.bmp
Red channel
Green channel
Blue channel
700
800
900
1000
1100
1200
1300
0
50
100
150
200
250
300

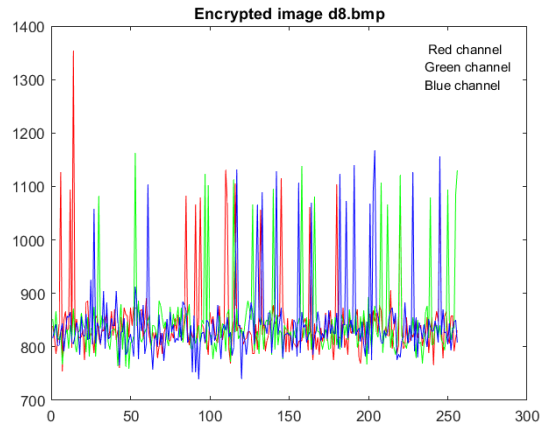


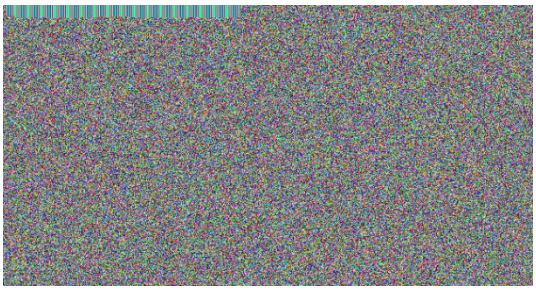

Original image d7.bmp
Red channel
Green channel
Blue channel
0
1000
2000
3000
4000
5000
6000
7000
8000
0
50
100
150
200
250
300

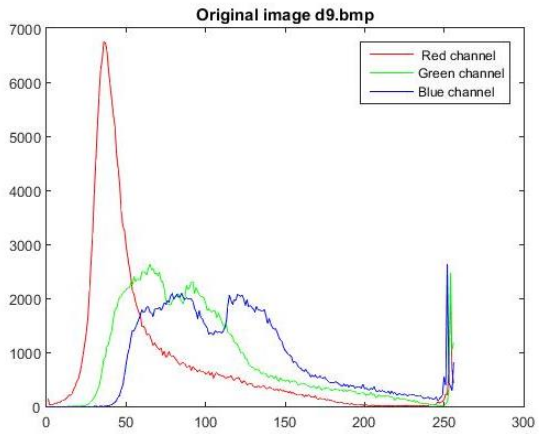

Encrypted image d7.bmp
Red channel
Green channel
Blue channel
700
800
900
1000
1100
1200
1300
1400
1500
1600
0
50
100
150
200
250
300

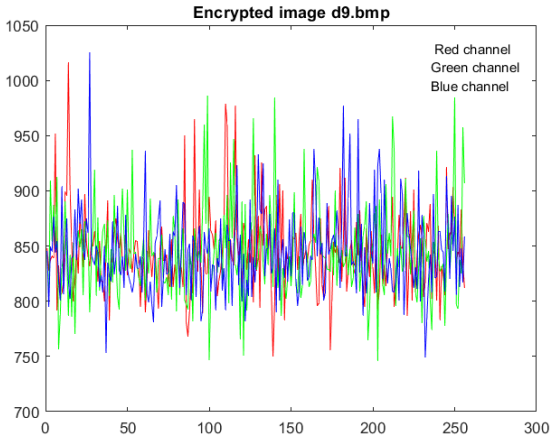


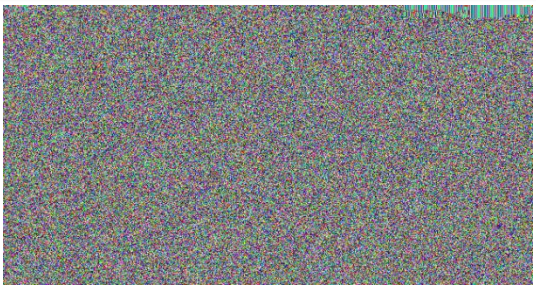

Original image d8.bmp
Red channel
Green channel
Blue channel
7000
6000
5000
4000
3000
2000
1000
0
0
50
100
150
200
250
300

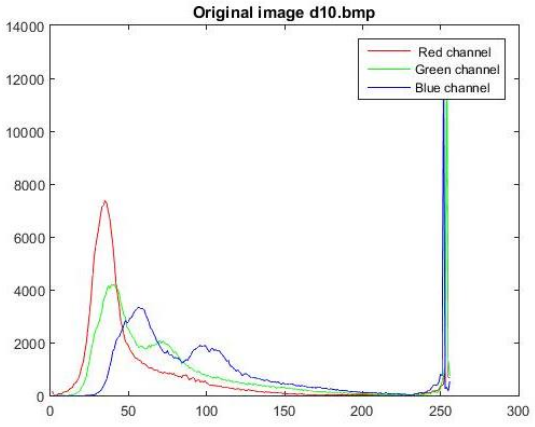

Encrypted image d8.bmp
Red channel
Green channel
Blue channel
1400
1300
1200
1100
1000
900
800
700
0
50
100
150
200
250
300

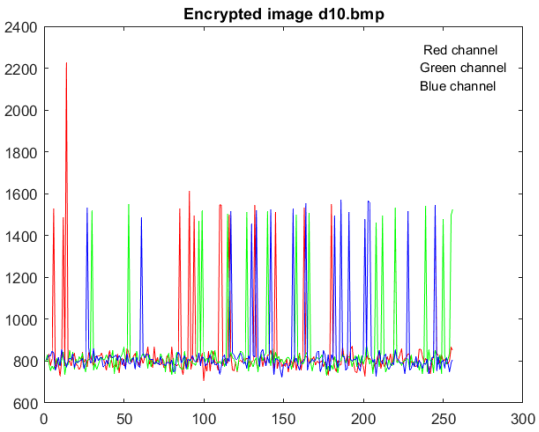


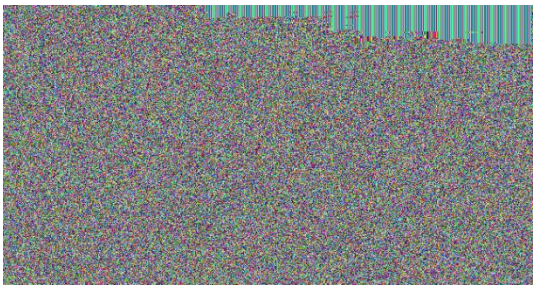

Original image d9.bmp
Red channel
Green channel
Blue channel
7000
6000
5000
4000
3000
2000
1000
0
0
50
100
150
200
250
300

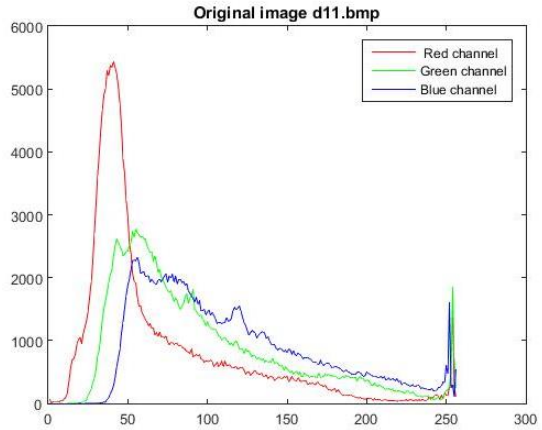

Encrypted image d9.bmp
Red channel
Green channel
Blue channel
1050
1000
950
900
850
800
750
700
0
50
100
150
200
250
300

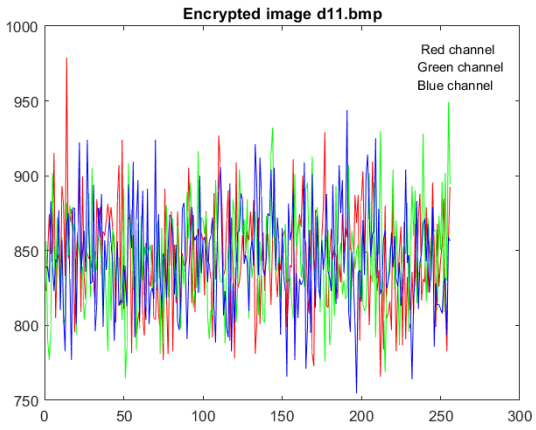


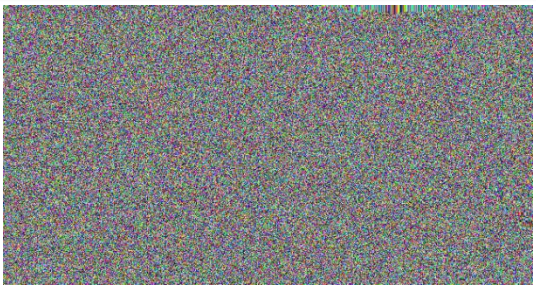

Original image d10.bmp
Red channel
Green channel
Blue channel

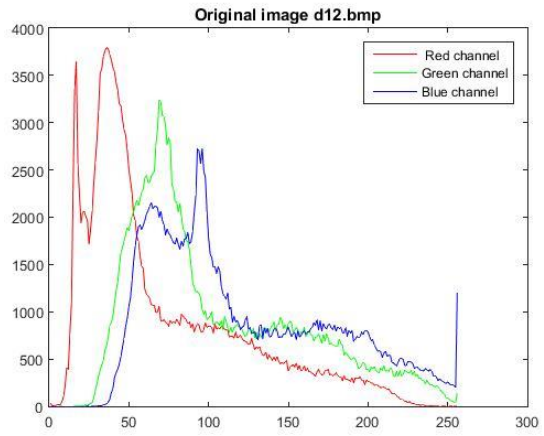

Encrypted image d10.bmp
Red channel
Green channel
Blue channel

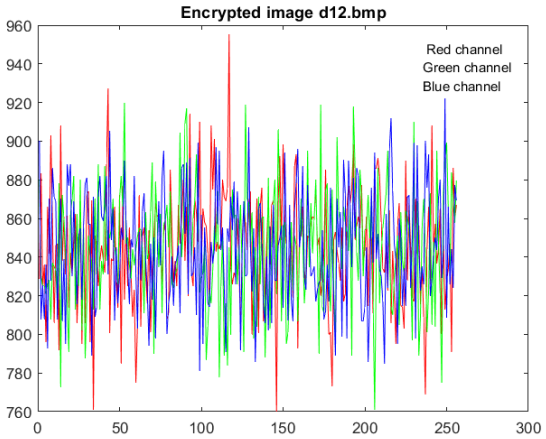


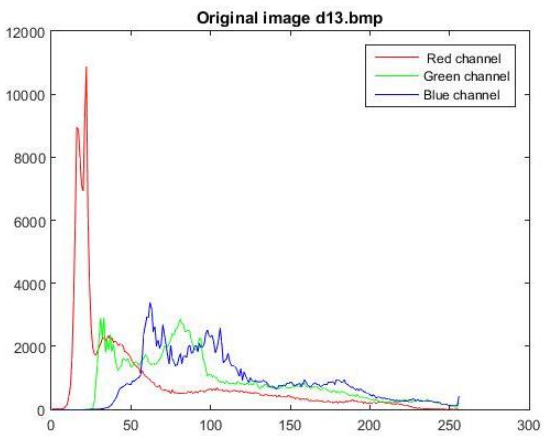

Original image d11.bmp
Red channel
Green channel
Blue channel

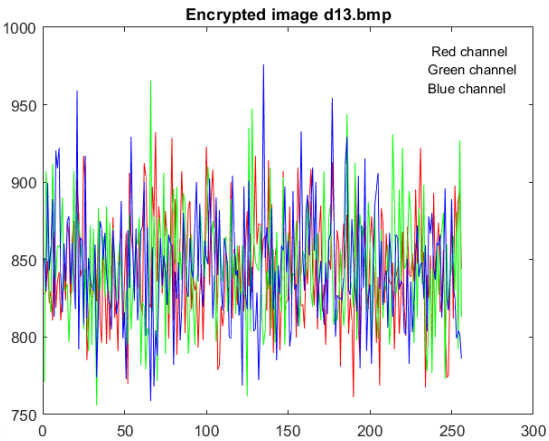

Encrypted image d11.bmp
Red channel
Green channel
Blue channel

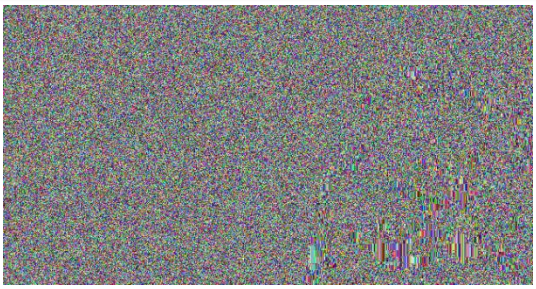


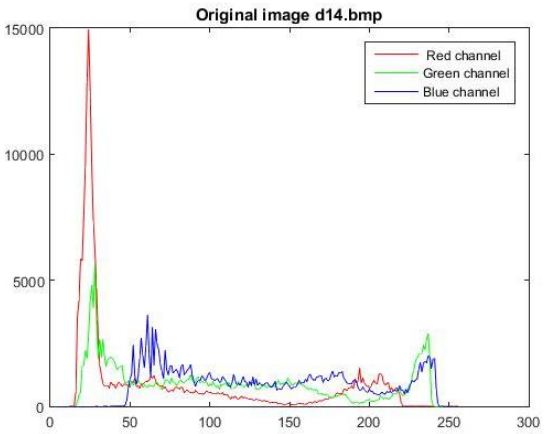

Original image d12.bmp
Red channel
Green channel
Blue channel

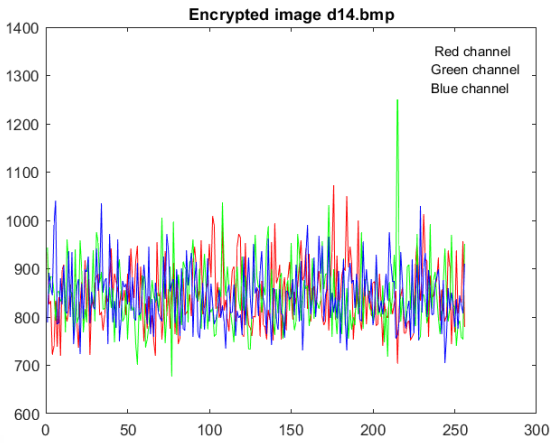

Encrypted image d12.bmp
Red channel
Green channel
Blue channel


Original image d13.bmp
Red channel
Green channel
Blue channel


Encrypted image d13.bmp
Red channel
Green channel
Blue channel

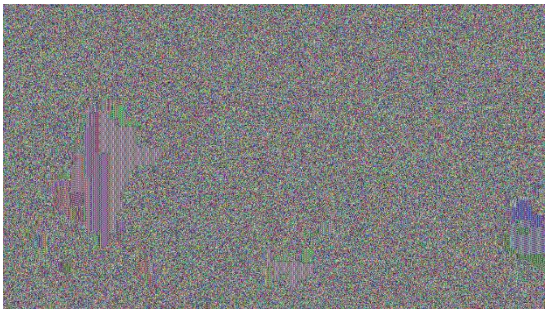


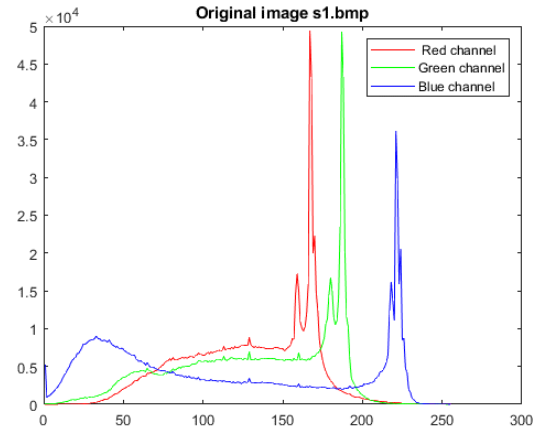


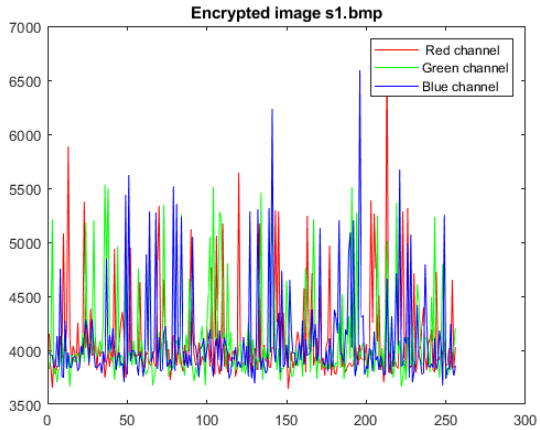


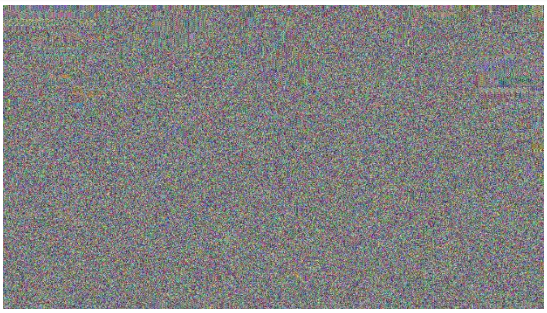
Και οι λήψεις του δεύτερου βίντεο το οποίο έχει περισσότερα χρώματα.

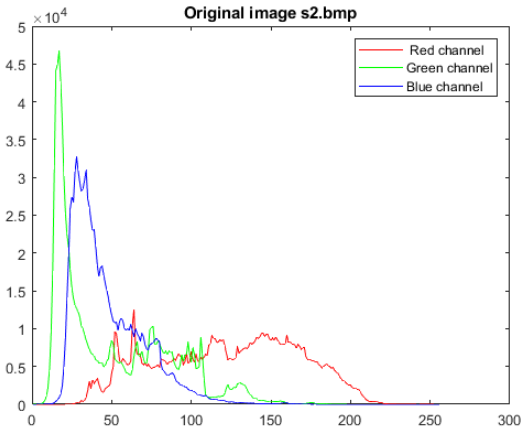
Εικόνες 32. Στιγμιότυπα αρχικού βίντεο, κρυπτογραφημένου και ιστογράμματά τους για το RGB

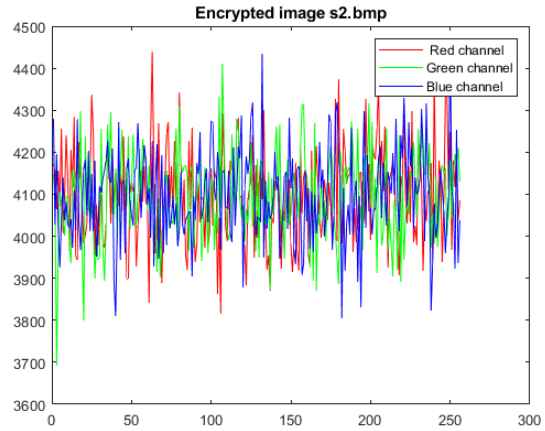


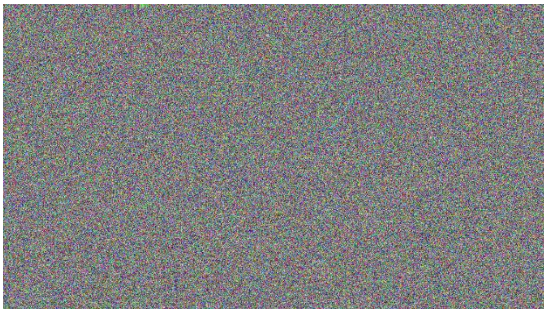


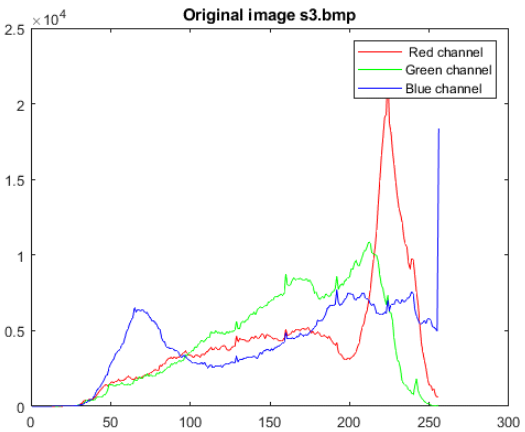


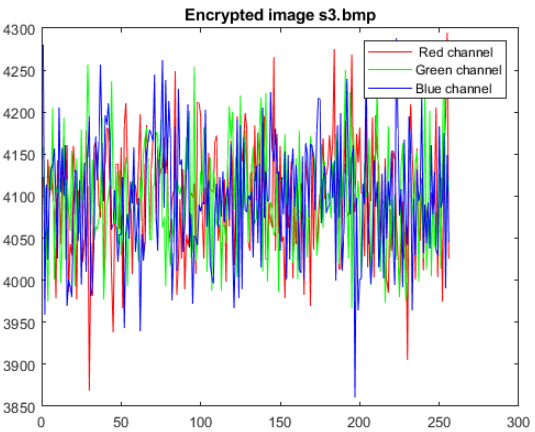


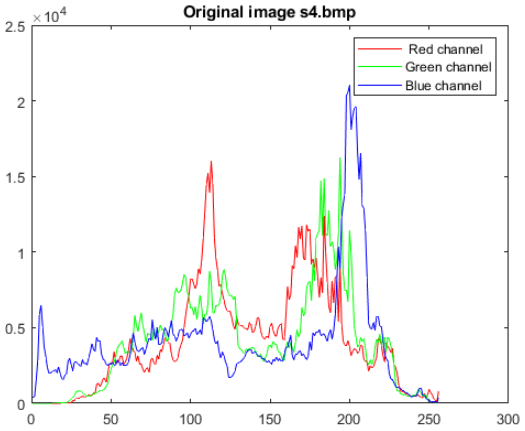

Original image s2.bmp
×10^4
Red channel
Green channel
Blue channel

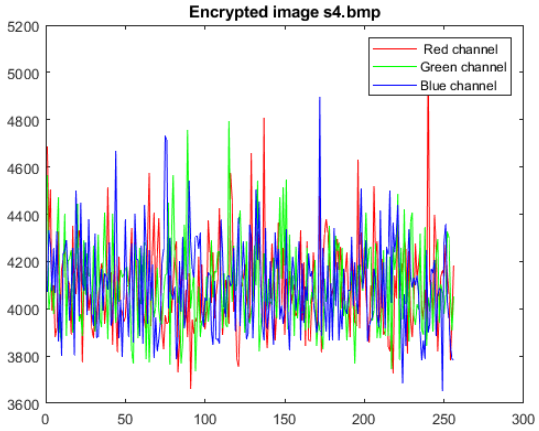

Encrypted image s2.bmp
Red channel
Green channel
Blue channel

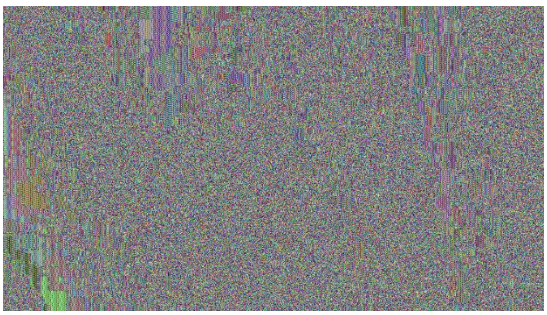


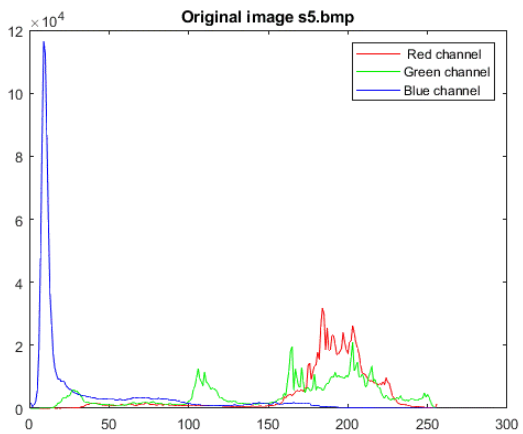

Original image s3.bmp
×10^4
Red channel
Green channel
Blue channel

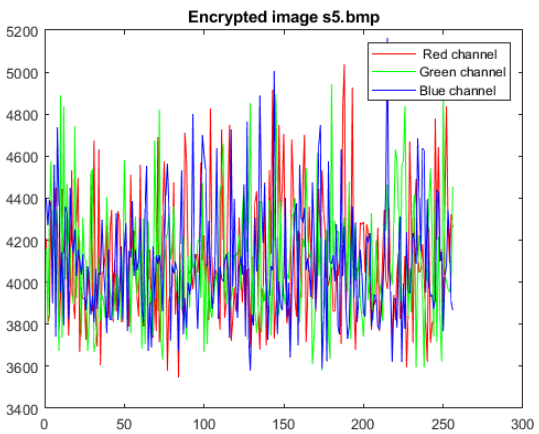

Encrypted image s3.bmp
Red channel
Green channel
Blue channel

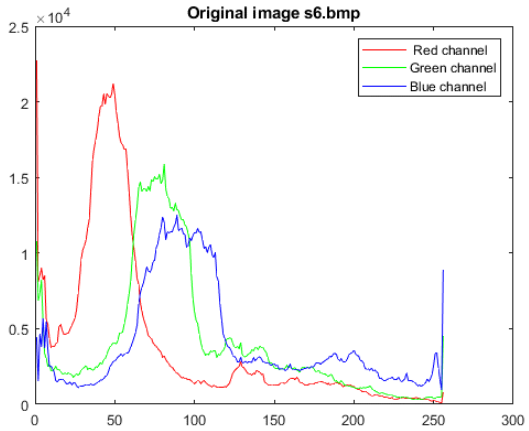

Original image s4.bmp
×10^4
Red channel
Green channel
Blue channel

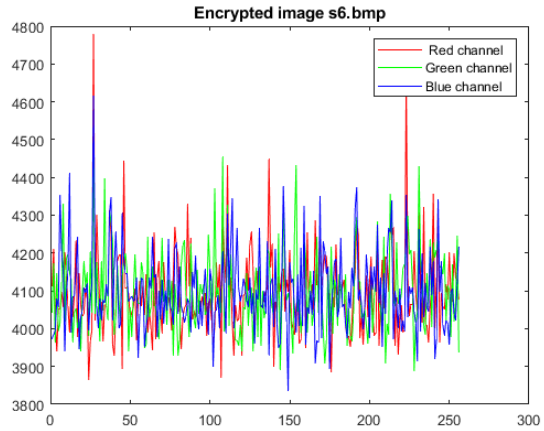

Encrypted image s4.bmp
Red channel
Green channel
Blue channel

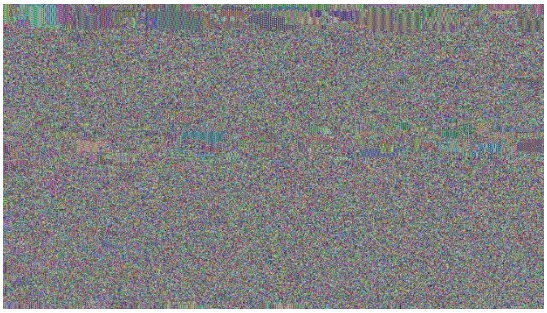


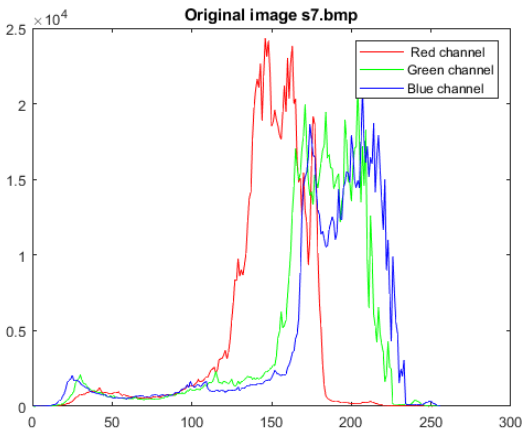

Original image s5.bmp
×10^4
Red channel
Green channel
Blue channel

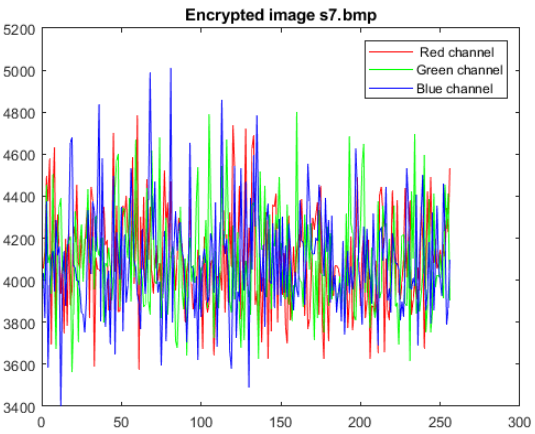

Encrypted image s5.bmp
Red channel
Green channel
Blue channel

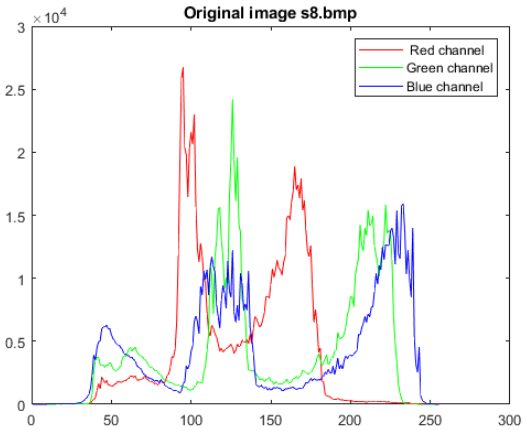

Original image s6.bmp
×10^4
Red channel
Green channel
Blue channel

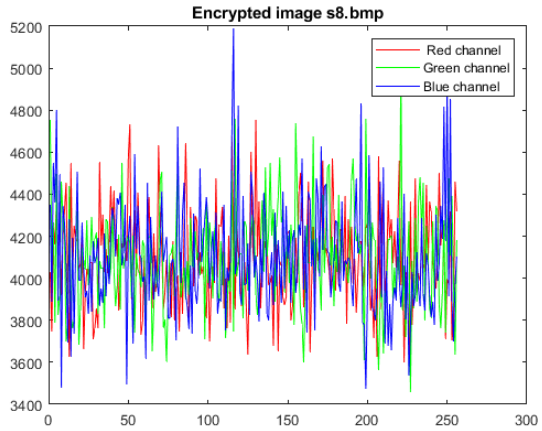

Encrypted image s6.bmp
Red channel
Green channel
Blue channel

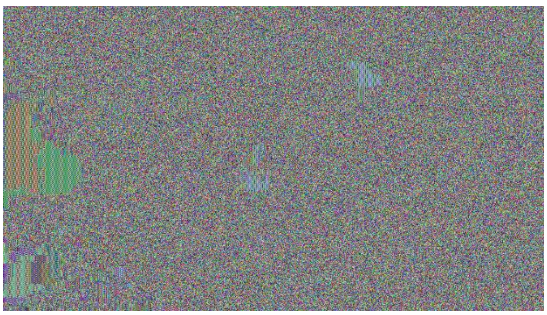


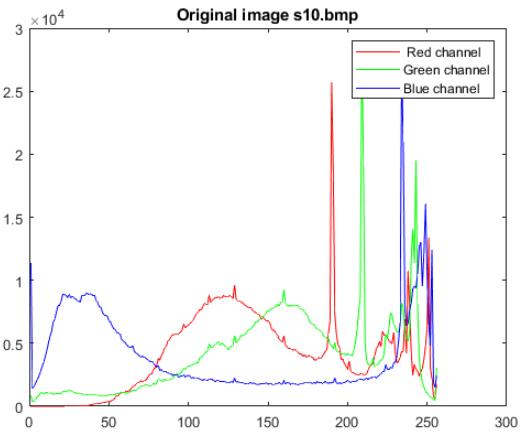

Original image s7.bmp
×10^4
Red channel
Green channel
Blue channel

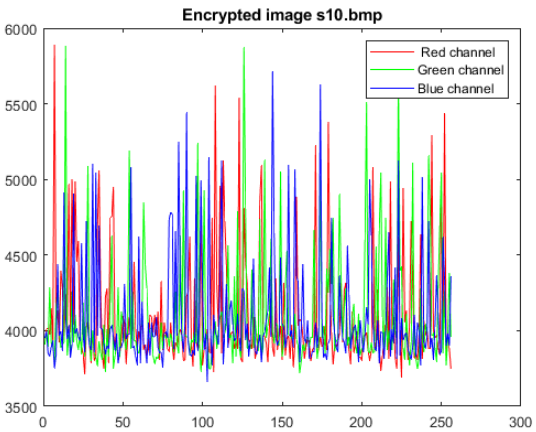

Encrypted image s7.bmp
Red channel
Green channel
Blue channel


Original image s8.bmp
×10^4
Red channel
Green channel
Blue channel


Encrypted image s8.bmp
Red channel
Green channel
Blue channel




Original image s10.bmp
×10^4
Red channel
Green channel
Blue channel


Encrypted image s10.bmp
Red channel
Green channel
Blue channel

6.3.2 Χρόνος κρυπτογράφησης και αποκρυπτογράφησης για διαφορετικά formats

Όπως φαίνεται από τις μετρήσεις του πίνακα 4, οι οποίες εξήχθησαν κατά τη διάρκεια της κωδικοποίησης και της αποκωδικοποίησης, τα βίντεο τύπου mp4, 3pg, mkv και f4v είναι τα γρηγορότερα.

Πίνακας 4. Χρόνος κωδικοποίησης και αποκωδικοποίησης

Μορφή (Format)	Χρόνος κωδικοποίησης (Msec)	Χρόνος αποκωδικοποίησης (Msec)
mpg	522	337
mp4	280	158
avi	478	343
wmv	654	323
3gp	124	106
mkv	277	171
flv	302	128
f4v	108	100

6.3.3 Ρυθμός μετάδοσης (bitrate)

6.3.3.1 Ρυθμός μετάδοσης αρχικού, κρυπτογραφημένου και αποκρυπτογραφημένου βίντεο

Υπολογίστηκε ο ρυθμός μετάδοσης (bitrate) για το αρχικό, το κρυπτογραφημένο και το αποκρυπτογραφημένο βίντεο για τα εξής formats: mpg, mp4, avi, 3gp, mkv, flv, f4v. Ο αλγόριθμος AES-128 κάνει πλήρη κρυπτογράφηση (100%). Ο τύπος που υπολογίζει το μέγεθος των δεδομένων και την αύξησή τους κατά τη μετάδοση είναι (Wikipedia):

Μήκος κωδικοποιημένου=Μήκος μη κωδικοποιημένου+(Μέγεθος Block-(Μήκος μη κωδικοποιημένου Mod Μήκος Block) Mod Μήκος Block)

$$KM=MKM+(MB-(MKM \bmod MB) \bmod MB)$$

Όπου KM: Μήκος Κωδικοποιημένου

MKM: Μήκος Μη Κωδικοποιημένου

MB: Μέγεθος Block

Στην περίπτωση του AES-128 το μήκος του block είναι 16 bytes. Άρα αν υπολογίσουμε το μήκος του κωδικοποιημένου βίντεο όταν το μη κωδικοποιημένο (αρχικό βίντεο) είναι mp4:

KM=7120000+(16-(7120000 Mod 16) Mod 16)

KM= 7120000+(16 - 0 Mod 16)

KM=7120000+(16 Mod 16)

KM= 7120000+0

KM=7120000

Συνεπώς το μήκος του κωδικοποιημένου βίντεο είναι ακριβώς ίδιο με του μη κωδικοποιημένου. Αντίστοιχα το ίδιο ισχύει και στα υπόλοιπα formats, όπως φαίνεται και στον πίνακα 5. Τα μικρότερα αρχεία είναι τα 3gp, mp4, flv και f4v. Το αρχείο τύπου 3gp έχει το μικρότερο μέγεθος αλλά η ποιότητά του είναι εξαιρετικά χαμηλή και διάφοροι στόχοι εδάφους θα ήταν πολύ δύσκολο να ξεχωρίσουν. Τα mp4 και flv έχουν ακριβώς το ίδιο μέγεθος, ενώ το f4v αποδεικνύεται ως η καλύτερη λύση γιατί έχει μικρό μέγεθος, εξαιρετική ποιότητα και πολύ μικρότερο χρόνο κωδικοποίησης και αποκωδικοποίησης.

Πίνακας 5. Μέγεθος βίντεο και ρυθμός μετάδοσης

Μορφή (Format)	Μέγεθος αρχικού βίντεο (Mbytes)	Μέγεθος κρυπτογραφημένου (Mbytes)	Μέγεθος αποκωδικοποιημένου (Mbytes)	Ρυθμός μετάδοσης αρχικού (Mbps)	Ρυθμός μετάδοσης κρυπτογραφημένου (Mbps)	Ρυθμός μετάδοσης αποκρυπτογραφημένου (Mbps)
mpg	17	17	17	136.000.000	136.000.000	136.000.000
mp4	7,12	7,12	7,12	56.960.000	56.960.000	56.960.000
avi	13,3	13,3	13,3	106.000.000	106.000.000	106.000.000
wmv	16	16	16	128.000.000	128.000.000	128.000.000
3gp	2,4	2,4	2,4	19.200.000	19.200.000	19.200.000
mkv	8,82	8,82	8,82	70.560.000	70.560.000	70.560.000
flv	7,12	7,12	7,12	56.960.00	56.960.00	56.960.00
f4v	3,54	3,54	3,54	28.320.000	28.320.000	28.320.000

6.3.3.2 Ρυθμός μετάδοσης μεταξύ μόνο συμπιεσμένου (zip) και κρυπτογραφημένου συμπιεσμένου αρχείου διαφόρων formats

Όπως φαίνεται στο 6.3.3.1, το μήκος του κωδικοποιημένου βίντεο είναι ακριβώς ίδιο με του μη κωδικοποιημένου. Πρόκειται για λογικό αποτέλεσμα γιατί όταν γίνεται κρυπτογράφηση ενός ήδη κωδικοποιημένου αρχείου δεν αλλάζει η ποιότητα ή ο όγκος του σε γενικές γραμμές. Προκειμένου να φανεί καλύτερα η διαφορά τους ακολουθείται η διαδικασία:

Α) Στην πρώτη περίπτωση κρυπτογραφείται και θα συμπιέζεται (zip) το video

Β) Στη δεύτερη περίπτωση μόνο συμπιέζεται το βίντεο

Στο τέλος συγκρίνονται τα αρχεία Α και Β για όλα τα formats.

Πίνακας 6. Μέγεθος μόνο συμπιεσμένων και κρυπτογραφημένων-συμπιεσμένων αρχείων

Μορφή (Format)	Μέγεθος αρχικού βίντεο (Mbytes)	Μέγεθος κρυπτογραφημένου και συμπιεσμένου (Mbytes)	Μέγεθος συμπιεσμένου (Mbytes)
mpg	17	17	14,8
mp4	7,12	7,12	5,71
avi	13,3	13,3	9,44
wmv	16	16	13,2
3gp	2,4	2,4	2,29
mkv	8,82	8,82	8,74
flv	7,12	7,12	5,71
f4v	3,54	3,54	3,45

Διαπιστώνεται λοιπόν πως το κρυπτογραφημένο δεν μπορεί να συμπιεστεί περαιτέρω ενώ το αρχικό παρουσιάζει μια μικρή μείωση στο μέγεθος και ακολούθως στο bitrate, αφού το μέγεθος είναι βασικό του στοιχείο. Όπως και στο 6.3.3.1 φαίνεται ότι τα μικρότερα αρχεία είναι τα 3gp, mp4, flv και f4v, ενώ το f4v αποδεικνύεται ως η καλύτερη λύση γιατί έχει μικρό μέγεθος, εξαιρετική ποιότητα και πολύ μικρότερο χρόνο κωδικοποίησης και αποκωδικοποίησης.

6.3.4 Peak signal-to-noise ratio μεταξύ διαφορετικών formats

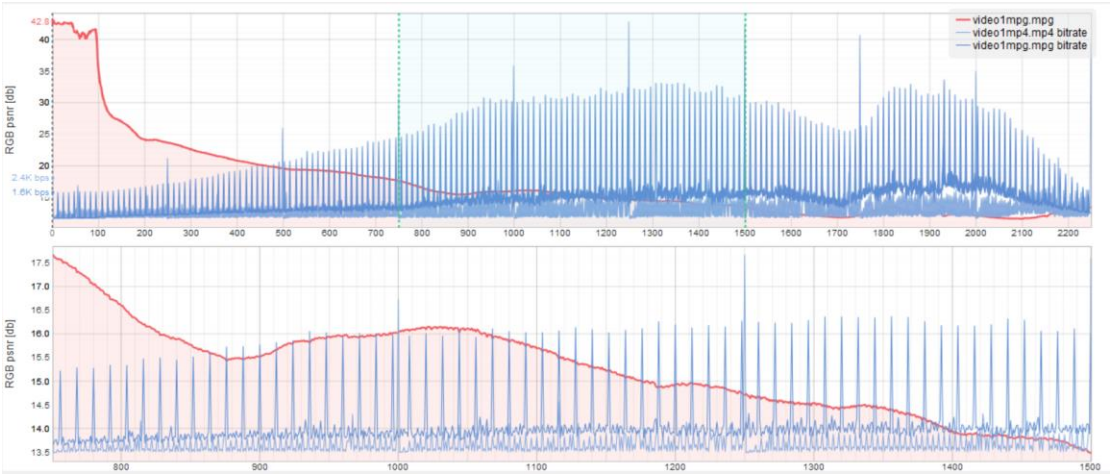
Τελευταία μέτρηση για να φανεί η διαφορά στον ρυθμό μετάδοσης μεταξύ των μικρότερων τύπων αρχείων είναι το Peak signal-to-noise ratio (PSNR). Ο όρος αυτός

αναφέρεται στον λόγο σήματος με θόρυβο που επηρεάζει τη αξιοπιστία της απεικόνισης και μετριέται σε dB. Ο τύπος του PSNR είναι:

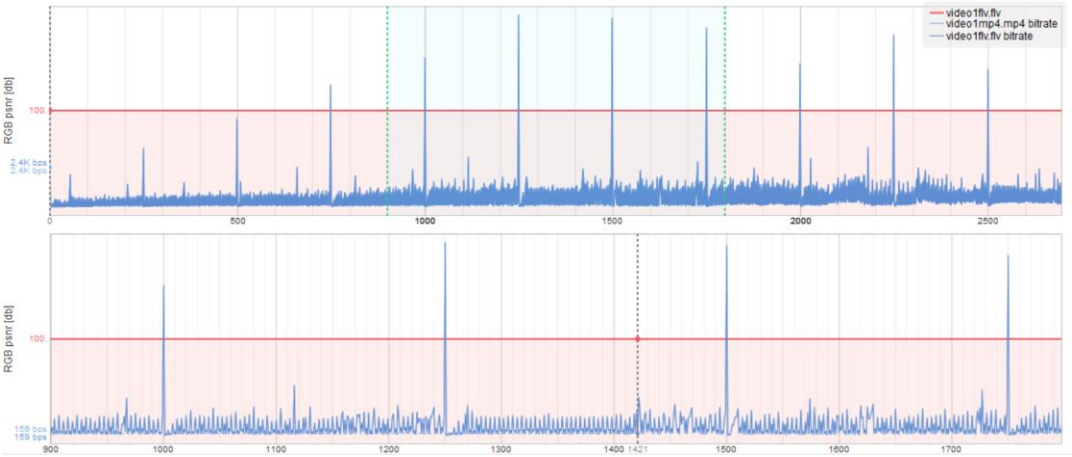
$$
\begin{aligned}
PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\
&= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\
&= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)
\end{aligned}
$$

Όπου MAX_I είναι η μέγιστη δυνατή τιμή των pixels της εικόνας και MSE (Mean Squared Error) είναι το Μέσο τετραγωνικό Σφάλμα (wikipedia).

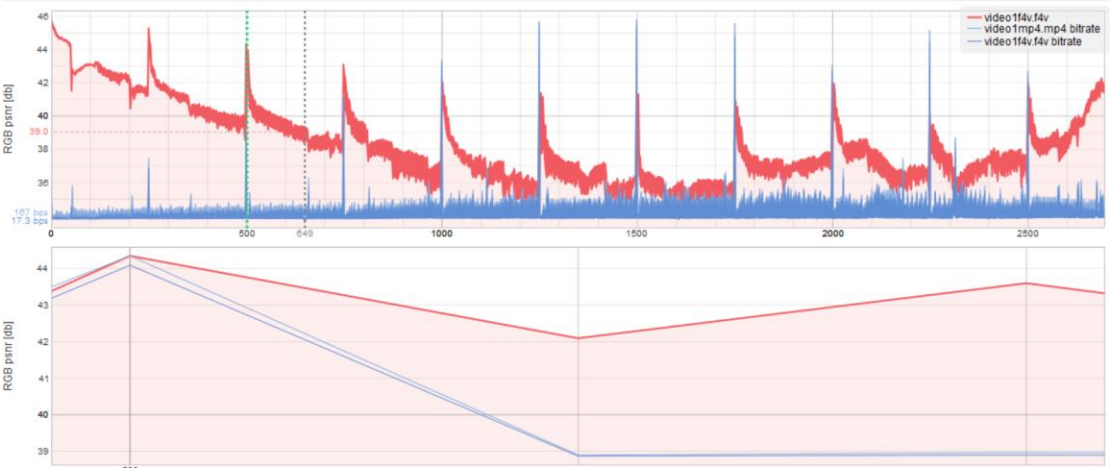
Στην πρώτη περίπτωση της σύγκρισης mp4 και mpg (Εικόνα 33) το mp4 έχει χαμηλότερο ρυθμό μετάδοσης ενώ στο PSNR μεταξύ mp4 και flv η κυματομορφή (Εικόνα 34) συμπίπτει γιατί τα αρχεία έχουν το ίδιο μέγεθος, αφού εξ αρχής οι δημιουργοί του flv στηρίχθηκαν στην κωδικοποίηση του mp4. Αντίθετα στη σύγκριση μεταξύ mp4 και f4v (Εικόνα 35) φαίνεται το πολύ χαμηλό bitrate του δεύτερου. Το ίδιο ισχύει και στη Εικόνα 36 όπου συγκρίνεται το mp4 με το mkv.



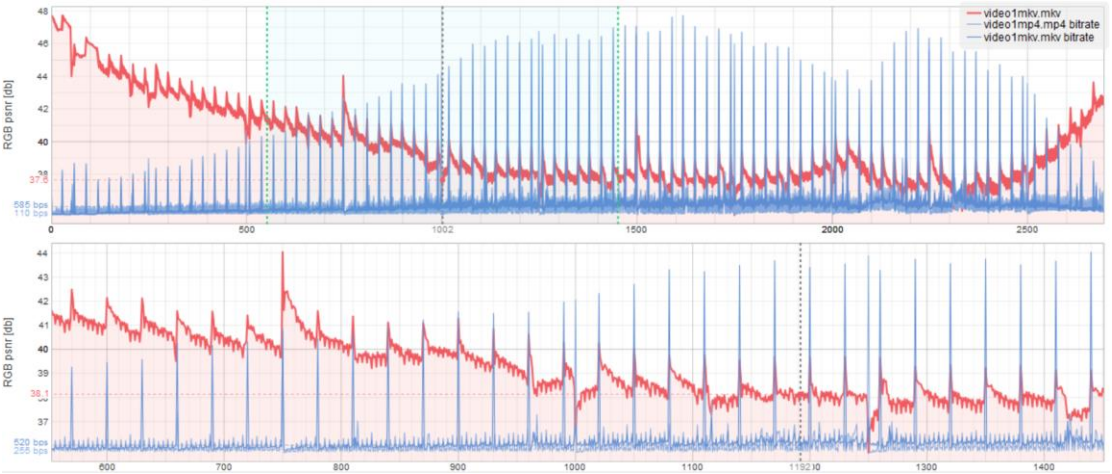
Εικόνα 33. PSNR mp4 και mpg



Εικόνα 34. PSNR μεταξύ mp4 και flv



Εικόνα 35. PSNR mp4 και f4v



Εικόνα 36. PSNR του mp4 και mkv

6.4 Αξιολόγηση των αποτελεσμάτων

Στην παρούσα εργασία επιλέχθηκε, σχεδιάστηκε και υλοποιήθηκε ένας ασφαλής και γρήγορος αλγόριθμος για κρυπτογράφηση πολυμεσικών δεδομένων από UAV (AES-128). Αφού παρουσίαστηκε με ιστογράμματα RGB η αποτελεσματικότητα του αλγορίθμου ως προς τα αρχικά και κρυπτογραφημένα βίντεο, ελέγχθηκε μεταξύ οκτώ formats ποιο έχει τον καλύτερο βαθμό συμπίεσης, ρυθμό μετάδοσης καθώς και χρόνο κωδικοποίησης και αποκωδικοποίησης, καταλήγοντας πως η καλύτερη επιλογή είναι ο τύπος f4v. Τέλος, μετρήθηκε ο λόγος σήματος προς θόρυβο (PSNR) μεταξύ των διαφορετικών formats, προκειμένου να επιβεβαιώσει τα συμπεράσματα για τη διατήρηση του ρυθμού μετάδοσης και την διατήρηση της ποιότητας του βίντεο μετά την κρυπτογράφηση.

7. Συμπεράσματα

Στην παρούσα εργασία μελετήθηκαν οι κυβερνοεπιθέσεις σε μη επανδρωμένα οχήματα και συγκεκριμένα, οι επιθέσεις στόχου (attack target), οι οποίες περιλαμβάνουν τις επιθέσεις στο κανάλι ελέγχου επικοινωνίας και στα δεδομένα βίντεο, τα οποία συλλέγονται από πολυμεσικούς αιθητήρες .
Αρχικά έγινε η ιστορική αναδρομή τόσο στη λήψη εικόνων/βίντεο όσο και στα μη επανδρωμένα οχήματα. Στη συνέχεια παρουσιάστηκαν οι βασικές κατηγορίες των UAV και αναλύθηκαν τα τηλεπικοινωνιακά τους μέρη. Έμφαση δόθηκε στη ζεύξη δεδομένων και τις λειτουργίες της, το είδος των σημάτων που διαχειρίζεται, τη διεπαφή του συστήματος, τις πιθανές καθυστερήσεις της διεπαφής και στα είδη και τις λειτουργίες των αισθητήρων. Η εργασία συνέχισε με περιπτώσεις επίθεσης σε UAV από τη διεθνή βιβλιογραφία, την ταξινόμηση των ειδών επιθέσεων, τους τρόπους ανίχνευσης της υποκλοπής των δεδομένων και δόθηκε έμφαση στις λογικές επιθέσεις, δηλαδή τις παρεμβολές του εχθρού προς το UAV. Στη συνέχεια του θεωρητικού μέρους, παρουσιάστηκαν και συγκρίθηκαν, βάσει συγκεκριμένων κριτηρίων, οι αλγορίθμοι κωδικοποίησης πολυμεσικών δεδομένων από διάφορους ερευνητές. Αυτοί ταξινομήθηκαν σε τέσσερις κατηγορίες. Τους αλγορίθμους κρυπτογράφησης όλων των επιπέδων, βάσει μετάθεσης, επιλεκτική και αντιληπτικής κρυπτογράφησης.

Στο δεύτερο μέρος της εργασίας σχεδιάστηκε και υλοποιήθηκε ένας αλγόριθμος AES-128, παρουσιάστηκε το διάγραμμα ενεργειών και τα διαγράμματα ροής. Ενώ παρουσιάστηκαν τα αποτελέσματα της αποδοτικότητας του αλγορίθμου. Παρουσιάστηκαν τμήματα τόσο του αρχικού βίντεο όσο και του κρυπτογραφημένου καθώς και τα διαγράμματα RGB τους, προκειμένου να φανεί το ποσοστό κρυπτογράφησης (100%). Επίσης, ελέγχθηκε ο χρόνος κρυπτογράφησης και αποκρυπτογράφησης για διαφορετικά formats βίντεο, ο ρυθμός μετάδοσης τους και ο λόγος του θορύβου (PSNR) μεταξύ των formats. Η εργασία έκλεισε με αξιολόγηση των αποτελεσμάτων του αλγορίθμου και τα γενικά συμπεράσματα.

Βιβλιογραφία

Ahmad Yousef, K. M., AlMajali, A., Ghalyon, S. A., Dweik, W., & Mohd, B. J. (2018) Analysis of Cyber- Physical Threats on Robotic Platforms. *Sensors (Basel, Switzerland), 18*(5), 11-12. doi:10.3390/s18051643

Agi, I., & Gong, L. (1996). An empirical study of secure MPEG video transmissions. In *Proceedings of Internet Society Symposium on Network and Distributed Systems Security* (pp. 137-144). IEEE.

Babatunde, A. N., Jimoh, R. G., & Abikoye, O. C. (2017). Survey of Video Encryption Algorithms. *Covenant Journal of Informatics and Communication Technology*, *5*(1).

Bergeron, C., & Lamy-Bergor, C. (2005). Complaint Selective encryption for H. 264/AVC video streams. In *2005 IEEE 7th Workshop on Multimedia Signal Processing* (pp. 1-4). IEEE.

Wang, C., Yu, H. B., & Zheng, M. (2003). A DCT-based MPEG-2 transparent scrambling algorithm. *IEEE Transactions on Consumer Electronics*, *49*(4), 1208-1213.

Chen, X., Makki, K., Yen, K., & Pissinou, N. (2009). Sensor network security: a survey. *IEEE Communications Surveys & Tutorials*, *11*(2), 52-73.

Deadliest Unmanned Killing Machines in USA Arsenal. (2011). Retrieved from https://tarwa.blogspot.com/2011/01/deadliest-unmanned-killing-machines-in.html

Dey, V., Pudi, V., Chattopadhyay, A., & Elovici, Y. (2018, January). Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study. In *2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)* (pp. 398-403). IEEE.

Fahlstrom, P. G. (2012). Data - Link Functions and Attributes. In P. G. Fahlstrom, *Introduction to UAV Systems, Fourth Edition* (p. 193). John Wiley & Sons, Ltd.

Spanos, G. A., & Maples, T. B. (1995). Performance study of a selective encryption scheme for the security of networked, real-time video. In *Proceedings of Fourth International Conference on Computer Communications and Networks-IC3N'95* (pp. 2-10). IEEE.

GoPro, (2018). The Ultimate GoPro. In F. t. R. G. F. You (Ed.), GoPro: GoPro.

Haring, L, (2018). Research, Development, Test and Evaluation Spotlight: Long-Range, Ultra-Long Endurance Unmanned Aircraft System. Retrieved fro http://coa/stguard.dodlive.mil/2018/01/rdte-spotlightlong-range-ultra-long-endurance-unmanned-aircraft-system/

Harris Corporation. (2009). Kgv-72 Type-1 Programmable Encryption Device. http://jproc.ca/crypto/kgv72.pdf

Hartman, K. (2013). The Vulnerability of UAV's to Cyber Attacks - An Approach to the Risk Assessment. *5th International Conference on Cyber Conflict.* Tallin: NATO CCD COE Publications.

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner, P. M. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In *Radionavigation laboratory conference proceedings*.

Hyperspectral Imaging. (2018). Hyperspectral Imaging, Retrieved from Hyperspectral Imaging. (2018). Hyperspectral Imaging, Retrieved from URL: http://www.sensorsinc.com/applications/military/hyperspectral-imaging/ Multispectral vs Hyperspectral Imagery Explained. (2018). Retrieved from https://gisgeography.com/multispectral-vs-hyperspectral-imageryexplained/

Jang, C. (2017). Taking Drones to The Next Level - Cooperative Distributed Unmanned - Aerial- Vehicular Networks for Small Drones and Mini Drones. *IEEE Vehicular Technology Magazine*, Volume 12, Issue 3, pp. 73-82.

Kakar, J. M. (2017). Waveform and Spectrum Management for Unmanned Ariel Systems Beyond 2025. Ithaca, New York: arXIv.org, Cornell University.

Kandangath, A. (2003). Jamming Mitigation Techniques for Spread Spectrum Communication Systems. Tempe, AZ: University of Arizona, Tech. Rep., 2003.

Tang, L. (1997). Methods for encrypting and decrypting MPEG video data efficiently. In *Proceedings of the fourth ACM international conference on Multimedia* (pp. 219-229).

Lian, S., Wang, X., Sun, J., & Wang, Z. (2004). Perceptual cryptography on wavelet-transform encoded videos. In *Proceedings of 2004 International Symposium on Intelligent Multimedia, Video and Speech Processing, 2004.* (pp. 57-60). IEEE

Lian, S., Wang, X., Sun, J., & Wang, Z. (2004). Perceptual cryptography on wavelet-transform encoded videos. In *Proceedings of 2004 International Symposium on Intelligent Multimedia, Video and Speech Processing, 2004.* (pp. 57-60). IEEE.

Lichtman, M., Jover, R. P., Labib, M., Rao, R., Marojevic, V., & Reed, J. H. (2016). LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation. *IEEE Communications Magazine*, *54*(4), 54-61.

Meyer and F. Gadegast, (1995). “Security Mechanisms for Multimedia Data with the Example MPEG-1 video” Project Description of SECMPEG, Technical University of Berlin.

Chen, M. (2014). A hierarchical security model for multimedia big data. *International Journal of Multimedia Data Engineering and Management (IJMDEM)*, *5*(1), 1-13.

Mohan, M. (2016). *Cybersecurity in drones* (Master dissertation, Utica College).

Mount, M., & Quijano, E. (2009). Iraqi insurgents hacked Predator drone feeds US official indicates. *CNN. com*Netanel R. B. 2020. Drone' Cryptanalysis:Smashing Cryptography with a Flicker, Singapore, 16-18 July

Nichols, R. K., Mumm, H. C., Lonstein, W. D., Ryan, J. J., & Carter, C. (2018). Unmanned Aircraft Systems (UAS) in the Cyber Domain: Protecting USA's Advanced Air Assets.

Ning, H., & Liu, H. (2012). Cyber-physical-social based security architecture for future internet of things. *Advances in Internet of Things*, *2*(01), 1.

Opall-Rome, B. (February 12, 2018). Israel Air Force says seized Iranian drone is a knockoff of US Sentinel, URL: https://www.defensenews.com/global/mideast-africa/2018/02/12/israel-air-force-says-seized-iraniandrone-is-a-knockoff-of-us-sentinel/

Pazarci, M., & Dipçin, V. (2002). A MPEG2-transparent scrambling technique. *IEEE Transactions on Consumer Electronics*, *48*(2), 345-355.

Pickholtz, R., Schilling, D., & Milstein, L. (1982). Theory of spread-spectrum communications-a tutorial. *IEEE transactions on Communications*, *30*(5), 855-884

Psiaki, M. L., O'Hanlon, B. W., Bhatti, J. A., Shepard, D. P., & Humphreys, T. E. (2013). GPS spoofing detection via dual-receiver correlation of military signals. *IEEE Transactions on Aerospace and Electronic Systems*, *49*(4), 2250-2267.

Schowengerdt, R. (2007). *Remote Sensing (Third edition).* Retrieved from Chapter 1: The Nature of Remote Sensing: http://www.springer.com/cda/content/document/cda_downloaddocument/9781461419938-c1.pdf

Schultz C. (2013). This Picture of Boston, circa 1860, Is the World’s Oldest Surviving Aerial Photo. Retrieved from https://www.smithsonianmag.com/smart-news/this-picture-of-boston-circa-1860-is-theworlds-oldest-surviving-aerial-photo

Scott, A. (2017). U.S. Army halts use of Chinese-made drones over cyber concerns. Reuters.

Shah, J., & Saxena, D. (2011). Video encryption: A survey. IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011

Shi, C., & Bhargava, B. (1998a). A fast MPEG video encryption algorithm. In *Proceedings of the sixth ACM international conference on Multimedia* (pp. 81-88).

Shi, C., & Bhargava, B. (1998b). An efficient MPEG video encryption algorithm. In *Proceedings Seventeenth IEEE Symposium on Reliable Distributed Systems (Cat. No. 98CB36281)* (pp. 381-386). IEEE.

Shi, C., Wang, S. Y., & Bhargava, B. (1999). MPEG video encryption in real-time using secret key cryptography. In *in Proc. Int. Conf. Parallel and Distributed Processing Techniques and Applications*.

Shunjun Li, Guanrong Chen, Albert Cheung, Bharat Bhargava, and Kwok-Tung Lo, "On the Design of Perceptual MPEG Video Encryption Algorithm", IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, No. 2, 2007,

Slagell, A. J. (2004). Known-Plaintext Attack Against a Permutation Based VideoEncryption Algorithm.

UAV Research Lab at the University of Sydney. (2018). Adapting UAV Control for Latency. UAV – Lab.

Wen, J., Severa, M., Zeng, W., Luttrell, M. H., & Jin, W. (2002). A format-compliant configurable encryption framework for access control of video. *IEEE Transactions on Circuits and Systems for Video Technology*, *12*(6), 545-557.

Whitlock, C. (June 20, 2014). When drones fall from the sky. https://www.washingtonpost.com/sf/investigative/2014/06/20/when-drones-fall-from-thesky/? noredirect=on&utm_term=.09b5d3e895bd

Wu, C. P., & Kuo, C. C. J. (2001, March). Fast encryption methods for audiovisual data confidentiality. In *Multimedia Systems and Applications III* (Vol. 4209, pp. 284-295). International Society for Optics and Photonics.

Xiao, C., Wang, L., Zhu, M., & Wang, W. (2016). A resource-efficient multimedia encryption scheme for embedded video sensing system based on unmanned aircraft. *Journal of Network and Computer Applications*, *59*, 117-125.

Young, D. (2018). Our eyes can play tricks on us but shortwave infrared (SWIR) imagery reveals all. Retrieved from URL: http://blog.digitalglobe.com/technologies/our-eyes-can-play-tricks-on-us-butshortwave

Βιβλιοθήκη του Louisville. (2018). Government Resources: Defense, Military, and Security https://library.louisville.edu/ekstrom/gov_defense/dronesmil

Αναδιώτης, Σ. (2018). *Η ανάπτυξη drones από την Τουρκία: προβλήματα, αντιμετώπιση, αποτροπή*. Διπλωματική εργασία. Διατμηματικό πρόγραμμα μεταπτυχιακών σπουδών στις διεθνείς σχέσεις και ασφάλεια. Πανεπιστήμιο Μακεδονία

Κόλλια, Β. (2017). *Μοντέλα επιθέσεων, μετρικές και προτεινόμενη ιεράρχηση μετρικών κυβερνοασφάλειας*. Διπλωματική εργασία Πανεπιστημίου Πατρών.

Λημνιώτης, Κ., 2020. Εργαστηριακό μάθημα κρυπτογραφίας https://docplayer.gr/41200800-Kryptografia-ergastiriako-mathima-2-3-4.html

https://stackoverflow.com/questions/9496447/encryption-of-video-files

https://stackoverflow.com/questions/26140389/facebook-conceal-image-encryption-and-decryption

https://uk.mathworks.com/matlabcentral/fileexchange/73037-matlab-aes-encryption-decryption-example

https://www.military.com/defensetech/2010/08/10/hezbollah-claims-it-hacked-israeli-drone-video-feeds

Παράρτημα 1

Για την υλοποίηση του αλγορίθμου χρησιμοποιήσαμε τις ακόλουθες σελίδες

https://stackoverflow.com/questions/9496447/encryption-of-video-files

https://uk.mathworks.com/matlabcentral/fileexchange/73037-matlab-aes-encryption-decryption-example

```
import java.io.File;
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.security.SecureRandom;
import java.security.spec.AlgorithmParameterSpec;
import javax.crypto.Cipher;
import javax.crypto.CipherOutputStream;
import javax.crypto.KeyGenerator;
import javax.crypto.NoSuchPaddingException;
```

```
import javax.crypto.SecretKey;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;

public class Encrypter {
    private final static int IV_LENGTH = 16; // Default length with Default 128
                                             // key AES encryption
    private final static int DEFAULT_READ_WRITE_BLOCK_BUFFER_SIZE = 1024;

    private final static String ALGO_RANDOM_NUM_GENERATOR = "SHA1PRNG";
    private final static String ALGO_SECRET_KEY_GENERATOR = "AES";
    private final static String ALGO_VIDEO_ENCRYPTOR =
"AES/CBC/PKCS5Padding";

    @SuppressWarnings("resource")
    public static void encrypt(SecretKey key,  AlgorithmParameterSpec paramSpec,
InputStream in, OutputStream out)
            throws NoSuchAlgorithmException, NoSuchPaddingException,
InvalidKeyException,
            InvalidAlgorithmParameterException, IOException {
        try {
            // byte[] iv = new byte[] { (byte) 0x8E, 0x12, 0x39, (byte) 0x9C,
            // 0x07, 0x72, 0x6F, 0x5A, (byte) 0x8E, 0x12, 0x39, (byte) 0x9C,
            // 0x07, 0x72, 0x6F, 0x5A };
            // generate new AlgorithmParameterSpec
            // AlgorithmParameterSpec paramSpec = new IvParameterSpec(iv);
            Cipher c = Cipher.getInstance(ALGO_VIDEO_ENCRYPTOR);
            c.init(Cipher.ENCRYPT_MODE, key, paramSpec);
            out = new CipherOutputStream(out, c);
            int count = 0;
            byte[] buffer = new byte[DEFAULT_READ_WRITE_BLOCK_BUFFER_SIZE];
            while ((count = in.read(buffer)) >= 0) {
                out.write(buffer, 0, count);
```

```
            }
        } finally {
            out.close();
        }
    }

    @SuppressWarnings("resource")
    public static void decrypt(SecretKey key,  AlgorithmParameterSpec paramSpec,
InputStream in, OutputStream out)
            throws NoSuchAlgorithmException, NoSuchPaddingException,
InvalidKeyException,
            InvalidAlgorithmParameterException, IOException {
        try {
            // byte[] iv = new byte[] { (byte) 0x8E, 0x12, 0x39, (byte) 0x9C,
            // 0x07, 0x72, 0x6F, 0x5A, (byte) 0x8E, 0x12, 0x39, (byte) 0x9C,
            // 0x07, 0x72, 0x6F, 0x5A };
            // read from input stream AlgorithmParameterSpec
            // AlgorithmParameterSpec paramSpec = new IvParameterSpec(iv);
            Cipher c = Cipher.getInstance(ALGO_VIDEO_ENCRYPTOR);
            c.init(Cipher.DECRYPT_MODE, key, paramSpec);
            out = new CipherOutputStream(out, c);
            int count = 0;
            byte[] buffer = new byte[DEFAULT_READ_WRITE_BLOCK_BUFFER_SIZE];
            while ((count = in.read(buffer)) >= 0) {
                out.write(buffer, 0, count);
            }
        } finally {
            out.close();
        }
    }

    public static void main(String[] args) {
        File inFile = new File("path\\file_name");
```

```
        File outFile = new File("path\\file_name ");
        File outFile_dec = new File("path\\file_name ");

        try {
            SecretKey key =
KeyGenerator.getInstance(ALGO_SECRET_KEY_GENERATOR).generateKey();
            byte[] keyData = key.getEncoded();
            SecretKey key2 = new SecretKeySpec(keyData, 0, keyData.length,
ALGO_SECRET_KEY_GENERATOR);
            byte[] iv = new byte[IV_LENGTH];

SecureRandom.getInstance(ALGO_RANDOM_NUM_GENERATOR).nextBytes(iv);
            AlgorithmParameterSpec paramSpec = new IvParameterSpec(iv);
// If  storing  separately
            Encrypter.encrypt(key,paramSpec, new FileInputStream(inFile), new
FileOutputStream(outFile));
            Encrypter.decrypt(key2,paramSpec, new FileInputStream(outFile), new
FileOutputStream(outFile_dec));
        } catch (Exception e) {
            e.printStackTrace();
        }

    }

}
```

Και για την επιλογή αρχείων διαφορετικών μορφών

```
import java.io.File;
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
```

```
import java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.security.SecureRandom;
import java.security.spec.AlgorithmParameterSpec;

import javax.crypto.Cipher;
import javax.crypto.CipherOutputStream;
import javax.crypto.KeyGenerator;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.SecretKey;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;
import java.util.Scanner;

public class Encrypter {
    private final static int IV_LENGTH = 16; // Default length with Default 128
                                             // key AES encryption
    private final static int DEFAULT_READ_WRITE_BLOCK_BUFFER_SIZE = 1024;

    private final static String ALGO_RANDOM_NUM_GENERATOR = "SHA1PRNG";
    private final static String ALGO_SECRET_KEY_GENERATOR = "AES";
    private final static String ALGO_VIDEO_ENCRYPTOR =
"AES/CBC/PKCS5Padding";

    @SuppressWarnings("resource")
    public static void encrypt(SecretKey key,  AlgorithmParameterSpec paramSpec,
InputStream in, OutputStream out)
            throws NoSuchAlgorithmException, NoSuchPaddingException,
InvalidKeyException,
            InvalidAlgorithmParameterException, IOException {
        try {
            // byte[] iv = new byte[] { (byte) 0x8E, 0x12, 0x39, (byte) 0x9C,
```

```
            // 0x07, 0x72, 0x6F, 0x5A, (byte) 0x8E, 0x12, 0x39, (byte) 0x9C,
            // 0x07, 0x72, 0x6F, 0x5A };
            // generate new AlgorithmParameterSpec
            // AlgorithmParameterSpec paramSpec = new IvParameterSpec(iv);
            long startTime = System.nanoTime();
    Cipher c = Cipher.getInstance(ALGO_VIDEO_ENCRYPTOR);
            c.init(Cipher.ENCRYPT_MODE, key, paramSpec);
            out = new CipherOutputStream(out, c);
            int count = 0;
            byte[] buffer = new byte[DEFAULT_READ_WRITE_BLOCK_BUFFER_SIZE];
            while ((count = in.read(buffer)) >= 0) {
                out.write(buffer, 0, count);
            }
    long endTime = System.nanoTime();
    long decryptiontime=(endTime-startTime)/1000000;
    System.out.println("Encryption time in miliseconds  : " + decryptiontime);
        } finally {
            out.close();


        }
     }


     @SuppressWarnings("resource")
     public static void decrypt(SecretKey key,  AlgorithmParameterSpec paramSpec,
InputStream in, OutputStream out)
            throws NoSuchAlgorithmException, NoSuchPaddingException,
InvalidKeyException,
            InvalidAlgorithmParameterException, IOException {
        try {
    long startTime = System.nanoTime();
            // byte[] iv = new byte[] { (byte) 0x8E, 0x12, 0x39, (byte) 0x9C,
            // 0x07, 0x72, 0x6F, 0x5A, (byte) 0x8E, 0x12, 0x39, (byte) 0x9C,
            // 0x07, 0x72, 0x6F, 0x5A };
```

```
            // read from input stream AlgorithmParameterSpec
            // AlgorithmParameterSpec paramSpec = new IvParameterSpec(iv);
            Cipher c = Cipher.getInstance(ALGO_VIDEO_ENCRYPTOR);
            c.init(Cipher.DECRYPT_MODE, key, paramSpec);
            out = new CipherOutputStream(out, c);
            int count = 0;
            byte[] buffer = new byte[DEFAULT_READ_WRITE_BLOCK_BUFFER_SIZE];
            while ((count = in.read(buffer)) >= 0) {
                out.write(buffer, 0, count);
            }
  long endTime = System.nanoTime();
  long encryptiontime=(endTime-startTime)/1000000;
  System.out.println("Decryption time in miliseconds  : " + encryptiontime);
        } finally {
            out.close();
        }
  }


   public static void main(String[] args) {
 Scanner scan= new Scanner(System.in);
 System.out.print("Please provide a videofile : ");
 String userfile = scan.nextLine();
        String[] filesplit=userfile.split("\\.");
 System.out.println(filesplit[0]+"."+filesplit[1]);
 File inFile = new File("path\\fine_name"+userfile);
        File outFile = new File("path\\fine_name"+filesplit[0]+"_enc."+filesplit[1]);
        File outFile_dec = new File("path\\fine_name \"+filesplit[0]+"_dec."+filesplit[1]);


        try {
            SecretKey key =
KeyGenerator.getInstance(ALGO_SECRET_KEY_GENERATOR).generateKey();
            byte[] keyData = key.getEncoded();
```

```
        SecretKey key2 = new SecretKeySpec(keyData, 0, keyData.length,
ALGO_SECRET_KEY_GENERATOR);

 //if you want to store key bytes to db  so its just how to recreate back key from bytes
array

        byte[] iv = new byte[IV_LENGTH];


SecureRandom.getInstance(ALGO_RANDOM_NUM_GENERATOR).nextBytes(iv);

        AlgorithmParameterSpec paramSpec = new IvParameterSpec(iv);

// If  storing  separately

        Encrypter.encrypt(key,paramSpec, new FileInputStream(inFile), new
FileOutputStream(outFile));

        Encrypter.decrypt(key2,paramSpec, new FileInputStream(outFile), new
FileOutputStream(outFile_dec));

   System.out.println("operation completed");

      } catch (Exception e) {

         e.printStackTrace();

      }


    }


}
```