JOURNAL OF AERONAUTICS AND SPACE TECHNOLOGIES
(ISSN : 1304-0448)
July 2021 Volume 14 Number 2
jast.hezarfen.msu.edu.tr

Research Survey

Comparison of Encrypted Image Transfer Approaches That Provide Secure Video Transfer for UAV Systems

Ebrar ŞAHİN[1] Ömer ÇETİN[2*]

[1] *National Defense University, Hezarfen ASTIN Space Sciences Department, 34149 Yeşilyurt, Istanbul, Turkey*, sahinebrar@outlook.com
http://www.orcid.org/0000-0002-3622-559X
[2] *National Defense University, Air NCO Vocational HE School, 35416 Gaziemir, İzmir, Turkey*, o.cetin@hho.edu.tr
http://www.orcid.org/0000-0001-5176-6338
* *Corresponding Author*

Article Info

Received: *May 19, 2021*
Accepted: *May 27, 2021*
Online: *July 26, 2021*

Keywords: Naive Algorithm, Selective Algorithm, Pure Permutation, Zigzag Permutation, Video Encryption, Security

Abstract

Today, Unmanned Aerial Vehicles (UAVs) become one of the leading technologies that are widely used for different purposes. Even though UAV systems are platform systems containing different hardware for a specific task, almost all UAV systems transmit real-time images to ground control stations (GCS). In this study it is aimed to review the methods included in the literature to ensure safe video transmission between UAV platforms and GCS and to compare their use in UAV systems by testing them on a scenario. Naive, Pure Permutation, Zigzag Permutation and Selective algorithm approaches that are among the widely used video encryption algorithms in the literature is selected as exemplary structures in this study, both because they need relatively low processing power and because they may be suitable approaches to real-time needs on mobile platforms. Within the scope of the study, a total of six performance criteria is determined and the algorithms are evaluated separately according to the performance criteria. As a result of the study, the most suitable solution for safe video transmission between UAV platforms and GCS is presented in a comparative perspective. The Selective Algorithm is selected among 4 methods examined as it is necessary to ensure the security of real-time image transfer in UAV systems as well as the fast communication between the UAV and GCS.

To Cite This Article: E. ŞAHİN, Ö. ÇETİN, "Comparison of Encrypted Image Transfer Approaches That Provide Secure Video Transfer for UAV Systems", Journal of Aeronautics and Space Technologies, Vol. 14, No. 2, pp. 169-176, July. 2021.

İHA Sistemleri için Güvenli Video Aktarımı Sağlayan Şifreli Görüntü Aktarım Yaklaşımlarının Karşılaştırılması

Makale Bilgisi

Geliş: *19 Mayıs 2021*
Kabul: *27 Mayıs 2021*
Yayın: *26 Temmuz 2021*

Anahtar Kelimeler: Naive Algoritması, Seçmeli Algoritması, Saf Permütasyon, Zigzag Permütasyon, Video Şifreleme, Güvenlik

Öz

Günümüzde İnsansız Hava Araçları (İHA) farklı amaçlar doğrultusunda yaygın olarak kullanımları artan öncü teknolojilerden birisi haline gelmiştir. İHA sistemleri belirli bir görev doğrultusunda farklı donanımlar ihtiva eden platform sistemleri olsalar dahi neredeyse tüm İHA sistemleri yer kontrol istasyonlarına (YKİ) gerçek zamanlı görüntü aktarımı yapmaktadırlar. Bu çalışmada İHA platformları ile YKİ arasında güvenli video iletimi sağlamaya yönelik literatürde yer alan yöntemlerin taramasının yapılması ve bunların bir senaryo üzerinde test edilerek İHA sistemlerinde kullanımlarının karşılaştırılması amaçlanmıştır. Literatürde yer alan ve yaygın olarak kullanılan video şifreleme algoritmaları arasından Naive, Saf Permütasyon, Zigzag Permütasyon ve Seçmeli algoritma yaklaşımları gerek nispeten düşük işlemci gücü ihtiyacı duymaları gerekse de mobil platformlar üzerinde gerçek zamanlı ihtiyaçlara yönelik uygun yaklaşımlar olabileceğinden bu çalışmada örnek yapılar olarak seçilmiştir. Çalışma kapsamında toplam altı adet başarım kriteri belirlenmiş ve algoritmalar performans kriterlerine göre ayrı ayrı uygulamalı olarak çalışma kapsamında değerlendirilmiştir. Çalışma sonucunda İHA platformları ile YKİ arasında güvenli video iletimi için en uygun çözüm karşılaştırmalı olarak ortaya konulmuştur. İHA sistemlerinde gerçek zamanlı görüntü aktarımının güvenliğinin sağlanması kadar İHA ile YKİ arasındaki iletişimin hızlı olması da gerektiğinden incelenen 4 adet yöntemin arasından Seçmeli Algoritma diğerlerinin önüne geçmiştir.

1. INTRODUCTION

Unmanned Aerial Vehicle (UAV) systems, whose potential benefits have initially been realized very late, have become rapidly widespread since the early 2000s, and the number and types of systems have increased rapidly, while at the same time their capabilities have been improved and their usage areas have increased considerably [1]. Depending on the fact that UAV systems offer more effective, economical, reliable, and safe solutions when they are compared to manned air platforms, satellites and various ground systems. Their application areas continue to expand. Military applications are the main usage areas of UAV systems for today [2]. Previously, UAV systems can only be capable of aerial imaging for reconnaissance purposes but now they can also carry out target detection and destruction. They perform aerial imaging with the help of different type of sensors on them. These are widely used electro-optical (EO) and infrared (IR) cameras and Synthetic Aperture Radar (SAR) systems [3]. In addition, hyper spectral and multi-spectral cameras are used within the scope of military applications. Image transfer should be done between platforms and Ground Control Stations (GCS) with minimum delay so that accurate and timely information can be delivered. Because of the data transmission between the UAV and the GCS is provided wirelessly and that video data sent via the wireless communication environment, it is accessible from anywhere, and it is possible that the data package in question will become available to unwanted persons [4]. Therefore, the security of transmitted images should be ensured using video encryption algorithms [5] [6]. Since the structures used in UAV systems are computers that consume low power and are equipped with relatively weak processors, effective image encryption algorithms that consume minimum computation power and fast algorithms (with the minimum delay) are discussed and compared in this study with practical examples.

In fact, the defined problem is not specific for the image transfer of UAV systems. The data packet sent by a sender over an online communication network, becomes accessible to third parties. For example, the data pack can be a concert video that someone sends it to his/her friend or real-time video from cameras in someone's smart home system, or it can also be a snapshot of a reconnaissance flight for a military operation. Therefore, third sides should be prevented from accessing images that do not belong to them by obtaining the data package, thus ensuring the security of both individuals and institutions and states. However, the main difference that distinguishes UAV systems from structures that require other encrypted image transfer is that the processors are relatively slower and low-power consumption structures. The delay is vital on UAV systems. Even if they are transmitted through end-to-end peer communication hardware, aerial broadcasting over long distances is likely accessible to a large number of unwanted receivers. The aim of this study is to secure data packets from other wireless devices by making them meaningless even if an infiltration attack is carried out by third parties [6].

In video encryption algorithms, factors such as security, time, format, and compression conformity are important. In an ideal real-time compression algorithm, the computation cost of encryption and decryption should not be too high. It should not affect the compression ratio. The format of the compressed video should be suitable for cutting, copying, and browsing.

Although there are many different examples of video encryption algorithms in the literature. In this study four different video encryption algorithms are selected, examined, and applied to achieve a comparison by using a computation structure that is similar with small size UAV system capabilities. In the second part of the study, metrics used in comparing image encryption algorithms are explained and their importance in the image transfer of UAV systems is examined. In the third section, how the examples of image encryption algorithms in the literature are determined and how the approaches evaluated as suitable for the image transfer of UAV systems work in a summary are explained together with their algorithms. In the fourth section, it is explained how to simulate a low-power mobile processor and an image transfer system to demonstrate the conditions as working on an UAV system, and it is stated how the selected approaches are run on this processor. Also, as a result of applied simulation, the results obtained by considering the performance criteria of the selected algorithms are compared. In the last section, it is explained in comparative perspective which approach is more suitable for UAV platforms and what can be done to make the approach even more suitable. Finally, all the results are discussed.

2. PERFORMANCE METRICS OF VIDEO ENCRYPTION ALGORITHMS

The performance metrics of the video encryption algorithms selected in the study are described in this section. When selecting video encryption algorithms, they are evaluated according to six different performance criteria [7]. In addition, the importance of these criteria for image transfer in UAV systems is explained under separate items:

Visual Distortion (VD): This criterion indicates how distorted the video obtained after the original video is. In some applications, visual distortion includes only a fraction. The attacker sees both the distorted image and the non-corrupted image. However, some sensitive data is subject to high visual distortion so that the attacker cannot see anything.

Encryption Rate (ER): A value found with the ratio of encrypted data to all data. This ratio should be minimized in order to avoid high process complexity.

Compression Friendly (CF): An encryption algorithm is considered compression-friendly if it has no effect on data compression efficiency or has little impact.

Format Compatibility (FC): Encrypted bitstream must be compatible with compressor. And the standard decoder should be able to decipher the encrypted bit stream without decrypting it.

Cryptographic Security (CS): Cryptographic security defines whether the encryption algorithm is safe from brute force and plain text attack. For multimedia applications, it is really important that the encryption algorithm provides cryptographic security.

Computation Speed (AS): The difference between encryption and decryption in real-time video applications should be quite short.

Each of the six criteria described is important for ensuring video security transmitted through UAV systems. Visual distortion, encryption rate, and cryptographic security metrics protect against the possibility that the image transmitted in UAV systems is captured by third parties. Speed is very important in real-time image transfers, the transfer between the UAV system and GCS must be fast so that the information contained in the image can be used in a timely manner.

3. VIDEO ENCRYPTION ALGORITHMS

Videos are transmitted through computer networks in various ways. Some are encrypted with different encryption methods, others are compressed and transferred with different codecs. Many video encryption algorithms are presented in the literature. This section describes the video encryption algorithms used for real-time image transfer [7].

3.1 Naive Technique

Each byte in the video is encrypted. Standards such as DES, RSA, IDEA and AES can be used as encryption techniques [8]. The basis of the Naive algorithm is that all video data is treated as text data. Because each byte is encrypted individually in the Naive algorithm. The visual corruption rate is high, the encryption rate is 100% as each byte is encrypted individually, and the cryptographic security varies according to the encryption standard used. In addition, since the compression process is done after the encryption process, it is compression friendly as it does not reduce the compression efficiency. The logic of the Naive technique in the form of pseudo-code is as follows:

```
FUNCTION naive_encryption (frame):
   FOR byte IN enumerate(frame):
        Create cipher
        Encrypt byte with cipher using AES
        standard
   END FOR
END FUNCTION
```

Figure 1. Pseudo-code of naive technique.

As can be seen from the above algorithm steps, the most important feature and advantage of the naive method used for image encryption is that it has a 100% encryption rate and provides high cryptographic security. The Naive algorithm uses encryption methods such as DES, AES, and RSA. The structure, called "cipher" in the so-called code, is an entity used in the encryption phase. This entity consists of the key and the type of encryption that will used when encrypting. The bytes are encrypted with this generated cipher.

3.2 Pure Permutation

The basis of this algorithm is to scramble the bytes of a certain frame of video data according to a certain permutation. This algorithm is vulnerable to plain-text attacks. Because the original version of the scrambled frame can be reconstructed by looking at other unscrambled frames. Based on this information, visual distortion may vary depending on how many frames are scrambled when the algorithm is examined. The encryption rate is 100%, the compression friendliness is 100% because it does not cause an increase in the data volume, but the encryption security is low because no encryption algorithm is used, it only scrambles the video frame, its speed is high. The logic of the pure permutation technique in the form of pseudo-code is as follows:

```
FUNCTION create(frame):
  Generate a list that include random indexes
  FOR x in frame:
    FOR y in x:
      FOR z in y:
       Assign byte to a temp value
       Swap byte with random index
       Assign temp value to random index
      END FOR
    END FOR
  END FOR
END FUNCTION
```

Figure 2. Pseudo-code of pure permutation.

As the pseudo-code above shows, each byte is relocated. The main advantage of this algorithm is that it is quite good regarding speed, but in terms of cryptographic security, the same cannot be said. If the list of random indexes is decrypted, the images are revealed.

3.3 Zigzag Permutation Algorithm

The zigzag permutation algorithm is different compared to the pure permutation algorithm. The reason for this difference is due to the construction of the permutation sequence created. In combinatorial mathematics, when each entry of the set {1, 2, 3, ..., n} is alternately greater or smaller than the previous input, it is called a zigzag permutation [9].

For example, the five alternate zigzag permutations of variable {1, 2, 3, 4} are as follows:

1, 3, 2, 4 → 1 < 3 > 2 < 4

1, 4, 2, 3 → 1 < 4 > 2 < 3

2, 3, 1, 4 → 2 < 3 > 1 < 4

2, 4, 1, 3 → 2 < 4 > 1 < 3

3, 4, 1, 2 → 3 < 4 > 1 < 2

When performance criteria are examined accordingly, visual distortion may vary, the encryption rate is 100%, it has no effect on encryption as compression is done after encryption, so it is compression friendly. Encryption security is low because the encryption standard is not used and bytes are scrambled according to a certain permutation. If there are frames that are not scrambled, the permutation can be solved from here. The logic of the Zigzag permutation technique in the form of pseudo-code is as follows:

```
FUNCTION create(frame):
  Create flag and assign 1 as value
  FOR x in frame:
    if frame[x] > frame[x+1]:
       swap(frame[x],frame[x+1])
  END FOR
END FUNCTION
```

Figure 3. Pseudo-code of zigzag permutation.

As can be seen from the algorithm steps above, the difference of the zigzag permutation method used for image encoding from pure permutation is that a random index list is not created. The bytes are swapped between one big and one small. It is faster than pure permutation.

3.4 Selective Algorithm

The selective algorithm does not encrypt each byte in the video data to reduce process complexity. The types of frames that must be known when encrypting video streaming are:

I- Frame (Intra coded frame) is an entire image, such as JPG or BMP image file. Frames P and B hold only a portion of image information (the section that changes between frames is important to them, they look at the previous second and the next seconds), so they need less space in the output file than an I-frame.
The P-Frame (Projected image, predicted picture) only keeps changes to the image compared to the previous frame. For example, in a scene where a car moves on a fixed background, only the movements of the car need to be encoded. The encoder does not need to store unchanged background pixels in its P-frame, thus saving space.
B- The frame (bidirectional predicted picture) saves even more space by using differences between the existing frame and both the previous and subsequent frames to determine its contents.
The algorithm can be used in 4 different ways:

1. All headers can be encrypted.
2. All headers and required frames can be encrypted.
3. All I-frames in frames P and B can be encrypted,
4. As in the Naive algorithm, all frames and each byte can be encrypted.

Visual distortion is high when evaluated according to performance criteria. The encryption rate will vary according to which of the 4 methods is selected, as mentioned above. If all frames are to be encrypted, then the encryption rate is 100%. It is compression friendly. Encryption security is high because one of the encryption standards is used. The speed varies according to which of the above 4 methods is selected. The logic of the selective algorithm working in the form of pseudo-code is as follows:

```
FUNCTION create(frame):
  FOR x in frame:
    FOR y in x:
      FOR z in y:
        if selectiveFunction() = 1
          create cipher
          encrypt byte with cipher
          swap(byte, encrypted byte)
      END FOR
    END FOR
  END FOR
END FUNCTION
```

Figure 4. Pseudo-code of selective algorithm.

Only selected bytes are encrypted, as seen in the pseudo-code block of the selective algorithm above. In this way, the level of encryption of the image depends mainly on the person who wrote the algorithm. The number of bytes selected, and the distortion rate of the image are directly proportional, and the speed is inversely proportional. The selective algorithm uses encryption methods such as DES, AES, and RSA [8] [10]. The structure, called "cipher" in the pseudo-code, is an entity used in the encryption phase. This entity consists of the key and the type of encryption that will used when encrypting bytes. The bytes are encrypted with this generated cipher.

4. COMPARISON OF VIDEO ENCRYPTION ALGORITHMS

The program is written to compare algorithms are encoded in Python 3.7. The algorithms described in the previous section are programmed and run on the Raspberry Pi 2 Model B with the Raspberry Pi OS operating system installed. The Raspberry Pi 2 Model B has 1 GB of RAM and a Quad Core CPU 900 MHz processor. The main reason for choosing this structure is the testing of the success of approaches under limited processing power and memory facilities and the effort to simulate the limited capabilities on the UAV.

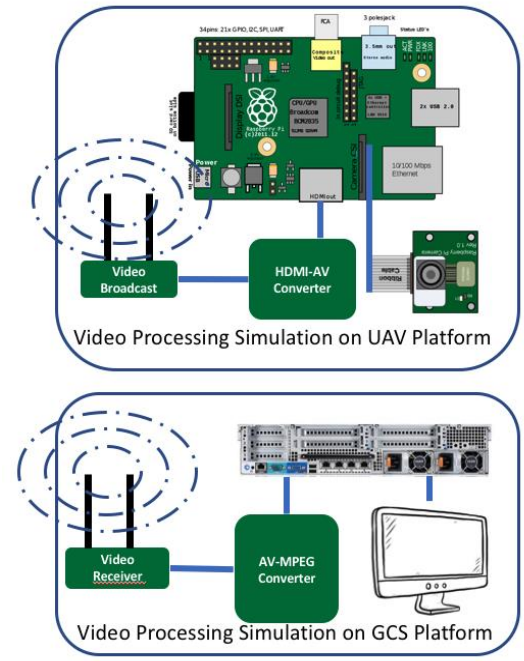

Figure 5. UAV- GCS simulation model.

The video stream is carried out with the model structure that appears in Figure 5. The image is encrypted with the camera on the Raspberry Pi and transferred to the video broadcaster.

In Figure 6 a sample image of the video frame obtained from the camera on the UAV platform and its form before encryption can be seen. This sample image will be presented to the reader under this section as a sample image frame to give an idea of the change during compressed video streaming using Naive Technique, Pure Permutation, Zigzag Permutation and Selective Algorithm methods.

Figure 6. Raw (Unencrypted) Image Frame Selected as Sample from Video Stream.

4.1 Naive Technique

Within the scope of the study, AES encryption standard is used when applying naive technique [11] [12]. The encrypted sample image frame output resulting from encrypting each byte in a frame is shown in Figure 7. If each byte in each frame is encrypted individually, the average time required to obtain this encrypted image on the hardware in question was 0.256 seconds after 270 frame image compression at a resolution of 320x240 pixels.

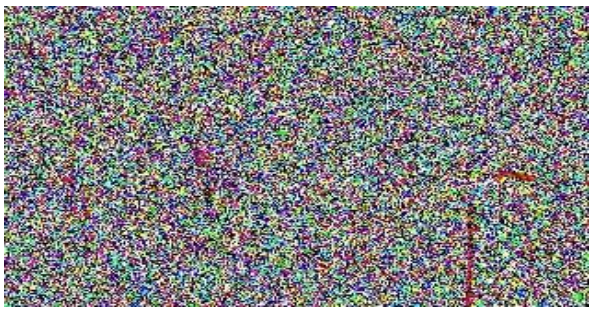

Figure 7. Sample image frame encrypted with AES.

With this technique, it is observed that a high visual distortion occurred, and the encryption rate is calculated as 100%. These images are compressed and transmitted in JPEG format and returned with 100% similarity on the receiving side.

4.2 Pure Permutation Algorithm

As a result of scrambling each byte in a video frame according to a certain permutation, as in the logic of the pure permutation algorithm, the result of the sample video frame on the streaming video as output is formed as in Figure 8.

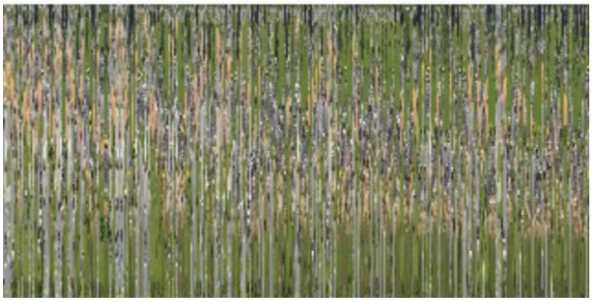

Figure 8. Sample image frame scrambled with pure permutation.

When the output image obtained by this technique is examined, the time required to obtain this scrambled image on the hardware in question was 0.12007 seconds after 270 frame image compressions at a resolution of 320x240 pixels. Quite a high visual distortion is occurred. This image is compressed and transmitted in JPEG format and returned with 100% similarity on the receiving side.

4.3 Zigzag Permutation Algorithm

According to the working logic of the zigzag permutation algorithm, the bytes should be sorted as one small and one large. To perform this process, each byte in the video frame is compared to the next byte. At the end of the algorithm, the scrambled image is as seen in Figure 9.

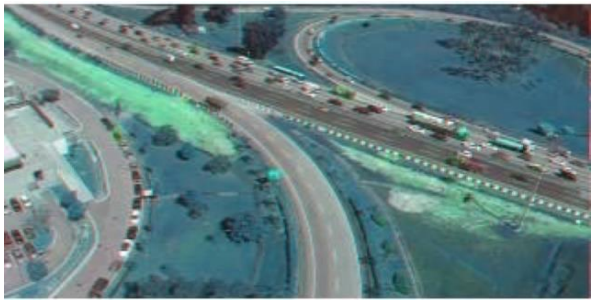

Figure 9. Sample image frame scrambled with zigzag permutation.

When the output image obtained with this technique is examined, the time required to obtain this encrypted image on the hardware in question is 0.0201 seconds as the average of the frame after 270 frame image compressions at a resolution of 320x240 pixels. It can be seen that a rather bad visual distortion has occurred. This image is compressed and transmitted in JPEG format and returned with a 50% similarity on the receiving side.

4.4 Selective Algorithm

To distort the overall structure of the image, a selection process was first made by modeling the indices of the height pixels. Because of being faster and higher in performance in compare to the asymmetric encryption algorithms such DES, AES encryption standard is used when applying selective algorithm [13].

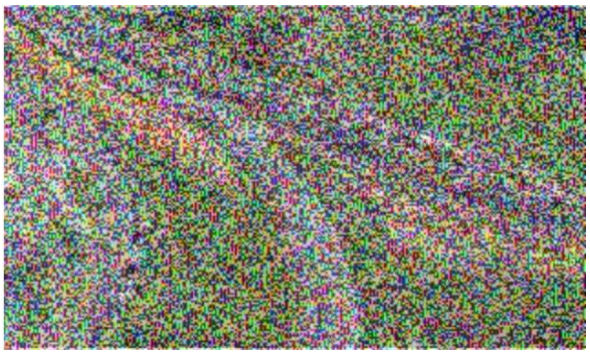

Figure 10. Image encrypted with selective algorithm.

If the mode is 0 according to the numbers 2 and 5, it is subject to encryption. As it can be seen in Figure 10, the general structure of the transferred image is distorted. If the number of bytes selected is reduced, it is understood even if the whole image is encrypted. This situation is as it appears in Figure 11.

When the output image obtained by this technique is examined, the time required to obtain this encrypted image on the hardware in question is 0.1276 seconds as the average of the picture frame for the relatively high byte-encrypted image process, which is shown in Figure 10, after 270 frame image compression at a resolution of 320x240 pixels, and 0.055 seconds for the image shown in Figure 11 and encrypted with relatively few bytes. While it is observed that a very high visual distortion occurs, the encryption rates are more than 50% for Figure 10 and Figure 11. This image is compressed and transmitted in JPEG format and returned with 100% similarity on the receiving side.

Figure 11. Fewer bytes of image encrypted with selective algorithm.

4.5 Comparison of Algorithm Performance

The algorithms are evaluated for each performance metric and shown in Table 1. Video comparison algorithms are applied tested on the same operating system and the described test hardware environment. The resolution of the sample video stream image set to 320x240 pixels. Visual distortion (VD) success is graded as high (H), low (L) and variable (V), encryption rate (ER) is expressed as a percentage rate, compression-friendly (CF), format compatibility (FC) and Cryptographic Security (CS) assessment is evaluated as positive (√) and negative (X). Computation speed (CS) evaluation being the duration of the encryption process per unit frame performed on the video stream consisting of 270 frames and is indicated in seconds.

Table 1. Performance Metrics.

Image Encryption Algorithm	**Performance Metrics**					
	VD	**ER**	**CF**	**FC**	**CS**	**CS**
Naive Technique	Y	%100	√	?	√	0.2567
Pure Permutation	Y	-	√	?	*X*	0.12007
Zigzag Permutation	D	-	√	√	*X*	0.0201
Selective Algorithm (The number of bytes encrypted is high)	D	D	√	*X*	√	0.1276
Selective Algorithm (The number of bytes encrypted is low)						0.0550

When the performance metrics are examined on the basis of the algorithms in Table 1, visual distortion

(VD) is quite high in Naive and Pure Permutation algorithms. This is because a process is performed on each byte in the video frame. However, in the selective algorithm, it is not known how the visual distortion will occur since the number of bytes to be encoded is variable, and the visual distortion differs in each video frame. In addition, visual distortion is not known in the Zigzag Permutation algorithm, since it is not known what kind of order the bytes will have when being relocated.

In terms of encryption rate (ER) [4], the encryption rate is 100% in the Naive technique because the ratio of encrypted bytes to other bytes is defined when the performance of the algorithms is evaluated. For other algorithms, the encryption rate either does not exist or is unknown. Pure Permutation and Zigzag Permutation algorithms do not have encryption so there is no encryption rate because the bytes are scrambled. The selective algorithm also selects bytes to encrypt. The encryption rate varies depending on how many bytes are encrypted.

Cryptographic security exists because encryption standards are used in the methods in which encryption is performed, but not if encryption standards are not used in methods where bytes are scrambled. Table 1 shows that there is cryptographic security in the Naive technique and selective algorithm, but the Pure Permutation and Zigzag Permutation techniques do not have cryptographic security because they scramble bytes, and the encryption standard is not used.

Computation speed is important in real-time secure image transfer. As shown in table 1, the method with the highest computational speed is the Zigzag permutation algorithm, while the algorithm with the lowest computational speed is the naive technique. The speed sequence is as follows: Zigzag, Selective (Number of encrypted bytes is low), Pure Permutation, Selective (Number of encrypted bytes is greater), Naive Technique. In the Zigzag Permutation algorithm, no encryption takes place, only the bytes are scrambled, but in the Naive technique, each byte is encrypted using the encryption standard.

5. CONCLUSION

Computation speed is just as important as encryption and security in real-time secure image transmission. Since each byte is encrypted individually in the Naive technique, the encryption rate is 100% and the image distortion rate is 100%, so that the encryption security is very high, but for real-time videos, the encryption and decryption speeds are as important as the reliability of the algorithm. With 0.2567 seconds as seen in Table 1, the Naive technique is the slowest technique. Therefore, it is slow for real-time image transfer. With the pure permutation algorithm, each byte in the video frame is scrambled using randomly determined permutation. Visual distortion may vary depending on how many bytes are scrambled, but if each byte is relocated, the image before the pure permutation algorithm cannot be understood from the algorithm applied image. Encryption security is not available because no encryption standard is used in the pure permutation algorithm. As seen in Table 1, the third fastest algorithm regarding computational speed is the Pure Permutation algorithm. Although the zigzag permutation algorithm is the best algorithm regarding computational speed, it does not distort the entire transmitted image. But since the bytes are constantly compared to each other and the bytes are relocated according to the comparison result, it is unknown what kind of sequence the bytes will have and how the visual distortion will be. Since visual distortion is unknown and no cryptographic security is available, zigzag permutation algorithm does not seem preferable for real-time secure image transmission. Since certain bytes of the video frame are selected and encrypted by the selective algorithm, the encryption rate is directly proportional to the selected bytes. In order to improve the duration, the number of bytes to be encrypted was reduced and the algorithm was tested, but when looking at the whole image, it was observed in Figure 11 that it did not distort the image. As a matter of fact, Table 1 clearly shows that the calculation speed slows down as the number of bytes increases. While the number of bytes to be encrypted is small, it is the 2nd fastest algorithm in regard to calculation speed, and the second slowest algorithm when the number of bytes to be encrypted is high.

It is obvious that there are many parameters for the selection of the ideal algorithm in real-time secure image transfer. Unfortunately, it is not possible for a single algorithm to perfectly meet all the criteria. For this reason, the most appropriate algorithm to be selected for encrypted image transfer, which provides secure video transfer for UAV systems, should ideally meet criteria such as encryption rate, cryptographic security, visual distortion and, most importantly, computational speed. If the optimal number of bytes to be encrypted for the selective algorithm can be found by looking at all the algorithms and the results examined in the study, both the desired visual distortion and encryption rate and the ideal calculation rate values can be reached. Thus, selective algorithm can be used as the ideal method for encrypted image transfer, which provides secure video transfer for UAV systems.

6. REFERENCES

[1] C. Karaağaç, "Geleceğin Harekât Ortamında İha Sistemleri:Askeri Uygulamalar & Teknoloji Gereksinimleri," in Havacılıkta İleri Teknolojiler Konferansı (HİTEK), 18-20 June, 2014.

[2] STM, *Geleceğin Hava Kuvvetleri 2016 – 2050*, 2016.

[3] H. Yao , R. Qin and X. Chen , "Unmanned Aerial Vehicle for Remote Sensing Applications—A Review," *Remote Sens*, vol.11, June 2019.

[4] W. Fan, Y. Wu, S. Ju, K. Zhang and W. Yang, "Secure UAV Communication with Robust Communication and Trajectory Design," in *International Conference on Computer, Information and Telecommunication Systems CITS 2019, Beijing, China, August 28-31, 2019.*

[5] M. Abomhara, O. Zakaria and O. O. Khalifa, "An Overview of Video Encryption Techniques," *International Journal of Computer Theory and Engineering*, vol. 2, pp. 103-110, February 2010.

[6] H. Kartik, A. Ashutosh, S. Tanay, G. Deepak and K. Ashish, "Hiding Data in Images Using Cryptography and Deep Neural Network," *Journal of Artificial Intelligence and Systems*, pp. 143–162, December 2019

[7] J. Shah and D. V. Saxena, "Video Encryption: A Survey," *IJCSI International Journal of Computer Science Issues*, vol 8, pp. 525-534, March 2011.

[8] Y. Li, "User Privacy Protection Technology of Tennis Match Live Broadcast from Media Cloud Platform Based on AES Encryption Algorith," in *IEEE 3rd International Conference on Information Systems and Computer Aided Education, Dalian, China, September 27-29, 2020*, pp. 267-269.

[9]Weisstein, Eric W. "Alternating Permutation." mathworld.wolfram.com From *MathWorld*--A Wolfram Web Resource. [Online]. Available: https://mathworld.wolfram.com/AlternatingPermutation.html [Accessed: May 27, 2021]

[10] A. Ajmera, M. Divecha, S. S. Ghosh, I. Raval and R. Chaturvedi, "Video Steganography: Using Scrambling- AES Encryption and DCT, DST Steganography," in *2019 IEEE Pune Section International Conference, Pune, India, December 18-20, 2019*, pp. 1-7.

[11] A. W. Dent and C. J. Mitchell, "Encryption," in *User's Guide to Cryptography and Standards*, 2004, pp. 45-71.

[12] W. Mao, "Basic Cryptographic Techniques," in *Modern Cryptography*, HP Books, 2004, pp. 203-243.

[13] A. Hamza and B. Kumar, "A Review Paper on DES, AES, RSA Encryption Standards," in *9th International Conference on System Modeling & Advancement in Research Trends, Moradabad, India, December 4-5, 2020*, pp. 333-338.

VITAE

Ebrar ŞAHİN received her B.Sc. degree in Computer Engineering from Faculty of Engineering, Fatih Sultan Mehmet Vakif University, Turkey in 2018. She is M.Sc. student in Cyber Security from NDU Hezarfen ASTIN, Turkey since 2018. She is currently working at National Research Institute of Electronics And Cryptology as R&D Engineer.

Dr. Ömer ÇETİN, is currently acting as assistant professor at the Computer Engineering Department of National Defense University (NDU), Turkey. He received his B.Sc. degree in Computer Engineering from Turkish Air Force Academy, Istanbul, in 2003. He received his M.Sc. degree in Software Engineering from Aeronautics and Space Technologies Institute (ASTIN), Istanbul, Turkey, in 2008. Asst.Prof.Dr. Ömer ÇETİN received his Ph.D. degree in Computer Engineering Program in Department of Computer Engineering of ASTIN in 2015. He is currently researching related with cyber security, deep learning, and autonomous systems.