Academic Science Journal

Random Keys Generating for Asymmetric Cryptography using Video Entropy

Rasha M. Mohsin*, Rasha I. ahmed, Saba Fouad Hassan

Collage of Computer Science, University of Technology, Baghdad, Iraq

*rasha.i.ahmed@uotechnology.edu.iq

Received: 13 April 2024 **Accepted: 18 August 2024**

Published: July 2025

DOI: https://dx.doi.org/10.24237/ASJ.03.03.855C

Abstract

After the widespread of the Internet and the emergence of multiple means of communication like Social media and email applications, the internet has become an integral part of our daily lives, whether practically or scientifically, in addition to other fields such as politics, trade, economics, and other fields. The rapid development in the field of communications has led to difficulties, such as finding methods for protecting transmitted data and difficulty of controlling data penetration. Public key encryption methods are considered the most suitable techniques for correspondence over the Internet, but there is a major problem facing most of the methods of this system, which is the methods of exchanging keys between the sender and the recipient. In this paper, a new technique for generating keys is proposed. By using some video properties to generate keys from data in the video randomly. The proposed method led to solve two problems at the same time. The first problem is the problem of exchanging keys, because sending the video via any means of communication does not raise the suspicion of the attacker, in addition to the difficulty of extracting the keys. The second problem is the methods of selecting the keys, because the proposed method generates many keys randomly.

The results present number and type of keys that generated, as shown in Table 1. These keys are strong for using in public key algorithms, in addition to the difficulty of guessing the keys

by attacker, because these keys are generated from a normal video that does not raise any suspicions in the attacker when exchanging them.

Keywords: Cryptography, asymptomatic key, video processing, entropy metric.

Introduction

In the modern era, with the spread of different types of information technology, communications and the need to transfer data from one point to another. Data transmission has increased rapidly with the rapid development of internet technologies and wireless communication. Institutions must have provided ways to share data via internet or any other communication medium in order to enable remote work. These institutions must provide appropriate security measures to share data and avoid many electronic attacks and data breaches. Therefore, many technologies are used to provide data security. One of these technologies is data encryption. However, current encryption methods still suffer from some difficulties because they contain some vulnerabilities that may allow electronic attacks to occur, especially when these data shared over the Internet [1].

Public-key encryption systems are one of the methods that used for digital signatures and encryption over the Internet, they use two types of keys: a public key for encryption and a private key for decryption. One of the basic steps is the key exchange between the sender and the receiver. This exchange is considered one of the greatest difficulties facing this method, as appropriate security measures must be provided. To exchange keys in addition to providing strong and difficult-to-guess keys [2].

In computer science, there are four types of data; text, image, audio and video. Each one of these file types has its own properties as well as uses. Nowadays the video file type is the most used among the other types, according to the latest statistics, and it may be transmitted [3].

All types of multimedia files can now be accessed freely and easily from any place using the internet. As a result, cryptographic techniques and security measurements are required to achieve a certain level of security and confidentiality during data storage and transmission [4].

Video can be defined as a visual representation of data. A video file is a representation of motion in the form of a sequence of images displayed in certain speed, therefor, the video file size is

large in size. Raw video can be structured as sequence of scenes, scenes as a sequence of scenes. Most of the presented work exploits this structure of video for segmentation and key-frame extraction [5].

In this paper we propose a system based on video mapping and characteristics to extract numbers with specific properties that are important in cryptography.

Related work

This section presents some work that studies methods to improve asymmetric cryptography or solve problems that aspect it by using multimedia (image, audio and video).

A. Mohsin, R. M., Ahmed, R. I and et al., suggest new methods to generate keys from a image generated by randome values, to be usee in key exchange protocol by applying two steps, the first step is to generate random image, and the second step extract keys from these generated image, the suggest system has two Weaknesses aspect, firstly, taking less time to be generate keys, secondly this method is exposed to attacks because the image generated raises the attacker's suspicion [6].

B. Sharma P et al.(2018), suggest a method to extract keys from images to improve the Diffie–Hellman protocol. They apply the XOR function between rows and columns that are equal to a multiple of eight in the matrix of the chosen image. This method has many weaknesses, firstly the method take convergent locations from selected image lead to be generate similar results, and therefore there is not flexibility if the user wants to replace the key when needed. Rather, the method must be repeated from the beginning, and this is a waste of time. Also suggest method is more chance vulnerable to attacks and the results are few [7].

C. Murali P and Palraj (2011) suggest a method to generate random keys by using a suggest generator called TRNG (true random number generator) based on row data from a selected image that must be sent between the sender and receiver. The proposed system is based on an image size of 25 x 25 pixel and type black and white to generate keys. Typically, this suggestion system was easy to implement and not expensive, but the small size of the image made it easy to attack as did the type of used image product [8].

Literature Review

This section includes a general view of important aspect that related to research topics.

Cryptography

One of the important techniques used for secure information transmitted via communications is a set of methods that depend mainly on converting into symbols or codes that can only be understood by the authorized person. Cryptography techniques depend on a set of mathematical concepts that differ according to the technology used. In general, it is divided into a set of mechanisms, the most important of which are [9]:

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Quantum Safe Cryptography and
- Cryptographic Hash Functions
- other

The main focus of this paper is on Asymmetric Key Cryptography. For more information about other methods, provide further information [9].

Asymmetric Key Cryptography

Asymmetric Key Cryptography is one of the Cryptography mechanisms that depends on the use of two interrelated keys, the first key is called a public key for encryption and the second key is call a private key for decryption, Figure 1 presents the asymmetric Cryptography process.

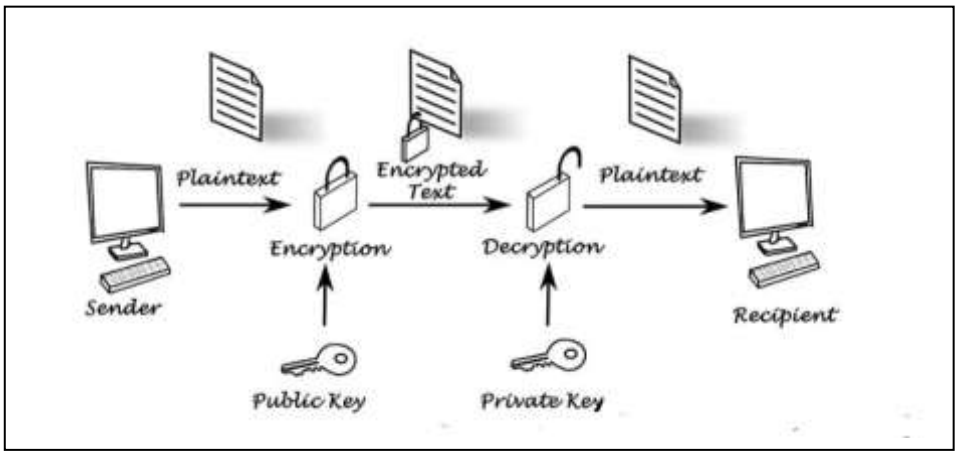

Figure 1: The asymmetric Cryptography process [10].

The public key encryption has been named this because it uses a set of mathematical functions called one-way functions. The public key encryption depends on the confidentiality of the private key, and in return, it is possible to distribute the public key through any means of communication.

Asymmetric Key Cryptography has various algorithms to implement this mechanism. Like the Diffie-Hellman key exchange protocol, Rivest Shamir Adleman (RSA), Digital Signature Standard (DSS) with Digital Signature Algorithm (DSA), TLS/SSL protocol, Elliptical Curve Cryptography (ECC) and many other algorithms.

Video Processing and Entropy Metrics

Video file represents a motion in the form of a sequence of images in different numbers, where the length of the video depends on the number of images. This leads to increase the size of the video file.

Video file type has many properties that can be used in many aspects, such as entropy. Entropy is an important measure in images as well as video, it represents the measurement of image content texture. Texture is a measurement of the properties of an image or video frame, such as coarseness, smoothness and regularity. When entropy value increases, details will not be visible to the human eye. Because of the high entropy areas, the human eye is insensitive to them. In other word, entropy is a statistical measure of randomness that is used to measure the texture of a video frame or an image [10]. The entropy can be calculated using equation (1) below, the entropy is represented as

$$E = -\sum P \log_2 (P) \quad (1)$$

Where P contained the histogram counts.

The Proposed System

The proposed system is designed to support encryption algorithms that operate based on the public key system, using video files and their properties to generate keys or numbers with specific characteristics. Depending on the target encryption algorithm. The amount of data that can be provided from the video is very large, while the video contains a set of forms, and each form contains a large set of data. In this proposed system, the frame is selected based on the entropy measure. The entropy measure provides a mechanism for selecting the frame that

contains a lot of data or the image in which the information is concentrated. Figure 2 shows the general diagram of the proposed system.

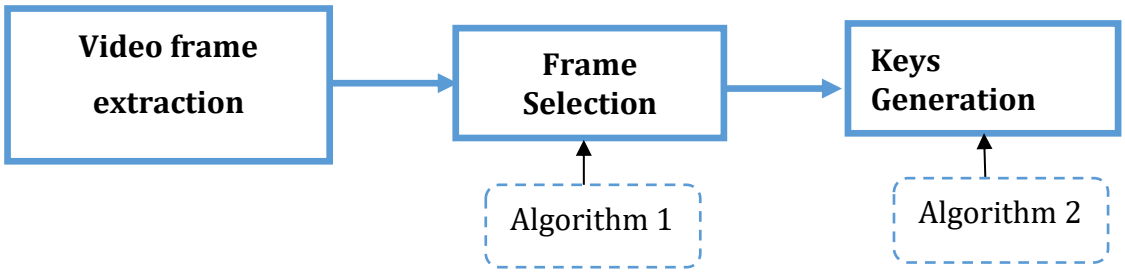

Figure 2: The general block diagram of the proposed system

The frame selection step presents how the frame can be selected from the video file, depending on the entropy measure from equation (1), Algorithm 1 illustrates the steps of frame selection.

Algorithm 1: Video Frame Selection
Input: video file Output: frame with max_entropy Step 1: read video file. Step 2: extract video properties (frame_count, frame_per_second(fps), frame_size …) Step 3: for var: 1 to frame_count read video_frame(var) calculate entropy (video_frame(var)) using equation(1) if entropy (video_frame(var)) > max_entropy then max_entropy= entropy (video_frame(var)) end for END

The next step is Keys generation that shows how can be generating keys from the frame that resulting from previous step. Algorithm 2 clarifies the steps of keys generation from the frame (primes number generation).

Algorithm 2: prime numbers generation(key generation)
Input: video frame ,count=1 Output: Vector of Prime Numbers, p, q Step1: convert extracted frame into array 2D called (A). Step2: Extract the primary diagonal from A , then put in vector P Step3: Extract the secondary diagonal from A , then put in vector S Step 4: v_length = length (p) Step5 : For i=1 to v_ Length Do

```
        V[i] = P[i] XOR S[i]    ……(2)
 End for.
Step6:: For i=1   to  V. Length Do
        If V[i] isprime then,
R[count]=V[i],
        Count=count+1
End if
        End for
End
```

Dataset

The proposed system was applied using the Waterloo QOE dataset [12]. This dataset consists of a set of videos (450 simulated streaming and 20 RAW HD) with a duration of an average of 13 seconds. This paper explains the results of applying the proposed system and discusse them based on 15 video samples out of the total database results. The 15 videos have been chosen for animals or nature because they have a high levels of property and thus the level of data is large.

Results and Discussion

We apply the proposed system on 15samples from the waterloo QOE dataset. After applying the steps, the results were according to the table (1)

Table 1: The proposed system results

Video sample	Video duration in seconds	No. of frames	Max frame entropy	Frame size	Time of frame extraction in seconds	Time of key generation in seconds	Number of primes in vector (v)	First large prime number (p)	Second large prime number (q)
Zap Highlight	13 s	250	7.4831	1920 x 1080	29.6590	64.614	222	1021	1019
Traffic And Building	12 s	297	7.5921	1920 x 1080	34.5430	63.93	195	1009	971
Valentines	13 s	233	7.5096	1920 x 1080	27.0109	67.35	226	887	839
Tears of Steel	13 s	239	6.9028	1920 x 1080	28.0948	63.8	196	991	1019

Slide Editing	13 s	250	6.7649	1920 x 1080	28.0160	64.02	202	971	997
Rush Hour	13 s	297	7.4155	1920 x 1080	32.3512	63.84	212	859	823
Puppys' Bath	13 s	235	7.5061	1920 x 1080	27.5301	66.35	219	1091	1021
Frozen Banff	13 s	232	7.8414	1920 x 1080	27.7781	63.64	167	1009	1021
CSGO	13 s	523	7.9418	1920 x 1080	64.9332	63.53	179	1009	1019
Bird-of Prey	13 s	300	7.8044	1920 x 1080	34.8799	63.3999	251	997	1013
FCB	13 s	297	7.3438	1920 x 1080	34.0892	63.65	176	991	1021
Mtv	13 s	219	7.0373	1920 x 1080	26.2145	64.88	199	967	1019
Frozen Banff	13 s	232	7.8414	1920 x 1080	27.7781	63.64	167	1009	1021
Tall Buildings	13 s	297	7.4016	1920 x 1080	34.5807	63.92	196	919	911
Roast Duck	13 s	299	7.8547	1920 x 1080	35.5402	63.84	215	983	1009

Table 1 illustrates the most important results extracted from the proposed system after applying it to the selected samples of videos, where it includes the frame that has the highest entropy after applying the equation (1) to it. In addition, Table contains the numbers of primes in vector (V), the two largest numbers within this frame and other information. When comparing the proposed system with previous works, it shows that, in the research (1), it suggests generating a random image as the first step and then generating keys. Generated. Generated. This method is exposed to attacks because the image generated raised the attacker's suspicion, Figure (3) illustrates an example of random image generation.

P-ISSN: 2958-4612
E-ISSN: 2959-5568

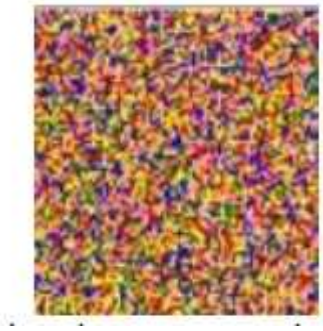

Figure 3: example of random image generation

In research (2), it was suggested that a small image (with 25 x 25 pixels and white and black colors) was used by key generation. The image size was fixed and small which facilitated the hacking process. While the size of the image has a major impact on security and complexity and thus delays in breaking and extracting the keys, as a result the increase in image size led to increased secrecy.

Table 2: Comparison table

authors	Image (NxN)	Time to generate P,Q(ms)	Extra time seconds
Proposed system	25x25	0.05	27.0109 to64.9332
MOHSIN,R,AHMED, R.I	25x25	0.049	-
Murali and Palraj	25x25	0.0003	-

The difficulty of breaking the key depends on generating methods for it, as the attacker's suspicion of the existence of the key is the first step in breaking the key. The result is based on assumption that the attacker knows that the keys exist.

Table 2 representing a comparison between the proposed system and two previous works, the table shows results that depend on the image size (because one of the researches adopted it (25x25) in addition to extra times. The comparison explain that our proposed system is considered better compared to the rest of the results because it is based on video, where the time of choosing the frame gives more strength and additional time to discover the keys.

Conclusion

The proposed system provides a secret way to generate prime numbers with specific properties such as randomness, unguessable and large value. The key generation based on video frames with the highest entropy. This would lead to an increase in security by distracting the attackers, the entropy measure would provide strength for the proposed system.

The proposed system can be used as a step in public key encryption and key exchange protocols because it provides a vector of prime numbers with large values. The results were discussed in the proposed system section and they increase security of key generation and authentication for key exchange.

Source of funding: None

Conflict of interest: None

Ethical clearance: None

References

[1] R. H. Marsaid, M. Huda, E. Laxmi Lydia, K. Shankar, Importance of Data Security in Business Management Protection of Company Against Security Threats, Journal of Critical Reviews, 7(1), (2020), DOI(https://doi.org/10.31838/JCR.07.01.45)

[2] S. Kallam, Diffie-Hellman: Key Exchange and Public Key Cryptosystems, Master degree of Science, Math and Computer Science, Department of India State University USA, 9/30/2015.

[3] B. Chandel, S. Jain, Video Steganography: A Survey, IOSR Journal of Computer Engineering (IOSR-JCE), 18(1), 11-17(2016), DOI(https://doi.org/10.9790/0661-18131117)

[4] J. Shah, V. Saxena, Video Encryption: A Survey, IJCSI International Journal of Computer Science Issues, 8(2), (2011)

[5] S. P. Algur, and R. Vivek, Video Key-Frame Extraction Using Entropy Value as Global and Local Feature, arXiv preprint arXiv:1605.08857, (2016), DOI(https://doi.org/10.48550/arXiv.1605.08857)

[6] R. M. Mohsin, R. I. Ahmed, R. Yaqub and S. Ethar, A new technique for Diffie-hillman key exchange protocol security using random image generation, In: 2019 First International Conference of Computer and Applied Sciences (CAS), Baghdad, Iraq, (2019), 262-267, DOI(https://doi.org/10.1109/CAS47993.2019.9075670)

[7] P. Sharma, D. Lakshman, Ch. BhargaviSravana and R. Pattanaik, A new technique of generating a key for Diffie-hellman algorithm, International Journal of Mechanical Engineering and Technology (IJMET), 9(1), 565–571(2018)

[8] P. Murali, and R. Palraj, True random number generator method based on the image for key exchange algorithm, International Symposium on Computing, Communication, and Control, (ISCCC 2009), 1, 85-88, (2011)

[9] Federal office of information security, Cryptographic Mechanisms: Recommendations and Key Lengths, January 9, (2023)

[10] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, A comparative survey of Symmetric and Asymmetric Key Cryptography, In: 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), Hosur, India, 83-93(2014), DOI(https://doi.org/10.1109/ICECCE.2014.7086640)

[11] S. Al-Rawi, A. T. Sadiq, B. Farhan, Digital Video Quality Metric Based on Watermarking Technique with Geffe Generator, Computer Science and Engineering, 2(7), 138-146(2012), DOI(https://doi.org/10.5923/j.computer.20120207.03)

[12] https://ece.uwaterloo.ca/~zduanmu/publications/tbc2018qoe/