EasyChair Preprint

№ 9617

V-Crypto Images/Videos/Texts by Two Key Authentication Using ACO Algorithm Technique

Janaki Raman Palaniappan

January 24, 2023

V-CRYPTO IMAGES/VIDEOS/TEXTS BY TWO KEY AUTHENTICATION USING ACO ALGORITHM TECHNIQUE

JANAKI RAMAN PALANIAPPAN

SOFTWARE PROFESSIONAL, USA

Email : Jackraman141987@gmail.com

Abstract

Everyone has a query, whether our data is safe when shared across internet services like emails, websites, apps and so on for a variety of purposes. Companies grub these data to extract the user needs and grow their business because this is one of the main strategies to taste the victory. This research discusses the unique method of protecting our own data ourselves before we send it. Cryptography is the method to secure the data and there are several methods and algorithms evolved in due course of time. After the research, I have come up with the unique cryptographic method that can encrypt and decrypt text files, images and videos. My method merges multi secret keys and 2 different techniques such as ACO algorithm and logical operation technique. A customer must provide two different secret keys as an input to encrypt and decrypt the data. Second key tells the distance of the path for the encryption to take place. This proposed method makes the encryption stronger as it is difficult for anyone to hack the data while decryption. The unique design algorithm helps the user to secure the data safely at source itself. This method has been experimented on multiple text files, images and videos.

Keywords

Ciphertext Cryptography, Visual Cryptography, Logical Operation Technique, ACO Algorithm

I. INTRODUCTION

Everyday people use variety of internet services like apps, email services, websites for a different purpose to share text files, video files and Images such as Tax documents, Passport, Driving License and so on which contains hypersensitive information that must be secured. Because organizations use these data to build up the future strategy of their business. It is a high time to keep our data safe and secure rather than to be a victim. Third party user who is not authorized accessing the data could lead to social problems.

In this Computer Age, we are surrounded by Internet all over the world and even monitored from space. Information is easily accessible in milliseconds from one end to another end of the world. But the major problem lies in the information security and authenticity when data is sent from source to destination.

This paper motive is to develop a unique method to protect the data at source. The developed method has a different technique that is combined of cipher cryptography, Video cryptography, two secret key authentication, ACO algorithm and logical operation technique that provides a unique way to encrypt and decrypt the data. This way we can make sure the data is protected at origin device itself.

II. CIPHERTEXT

Cryptography is the technique to secure information by transforming into a non-readable format and allows only expected users to view the content. This technique is widely used due to great security.

Ciphertext is the process of converting the plain text into an encrypted text using an algorithm. It will be non-readable until the text is decrypted to plain text using the key.

Widely used 2 methods of cryptography are,

Secret Key – Sender and receiver must use the same key to view the information. This method is also known as Symmetric Key.

Public Key – Sender would have Public Key and Receiver would have Private Key as it uses key pair technique to Encrypt and Decrypt the data. This is also known as Asymmetric Key.

Few methods of Cipher text are,

Substitution Cipher – Replace characters in the plain text with the alternate characters to produce cipher text.

Polygraphy Cipher – This method substitutes with two or more groups of letters because that masks frequency distribution of letters unlike above making much more difficult.

Transposition Cipher – This method rearranges the order of letters according to a specific algorithm like simple columnar algorithm writes the plain text in horizontal to vertical manner to produce cipher text.

III. VISUAL CRYTOGRAPHY

Visual Cryptography is a method that allows the images, videos and so on to encrypt and decrypt. Encrypt process converts the file into a non-readable format. Permissible user is allowed to decrypt the data. After decryption takes place, the file appears the original.

IV. ACO ALGORITHM

ACO algorithm (Ant Colony Optimization) is based on the ANT behavior to search for the food. They live in colonies. Ant hops to a different place randomly in search of food. Once the ant finds the source of the food, it starts depositing the markers on the path and goes back to the colony. It is based on the quality and quantity that other ants follow which path to choose. The other ants smell the markers and certainly follow the markers to reach the food. This optimizes the path to shorter for other ants to reach the destination.

V. ALGORITHM RESEARCH

Let it be a ciphertext cryptography or visual cryptography, there are many developed algorithm methods available in the market to secure the data. This research consists of a unique algorithm and will be handled to secure texts, images and videos with a different approach. This unique technique provides a very high security to the data.

Algorithm senses the input file automatically based on the extension of the file like .txt, .doc, .pdf, .png, .jpg, .mp4, etc., to know whether it must do a ciphertext or visual cryptography. Ciphertext cryptography handles all types of text related files and visual cryptography handles all types of images and videos.

Encryption process is a combination of multiple techniques such as cipher/visual input file, 2 secret key authentication, ACO algorithm technique and logical operation technique to secure the file. If third party wants to hack the file, then user must decode 2 secret keys. Secret keys make it more stronger for a third party to hack it.

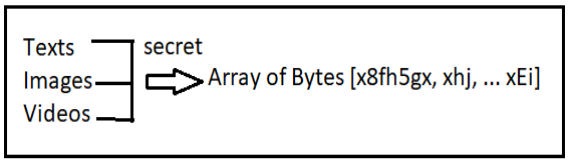


Figure 5.1 – Array of secret bytes

Encryption process goes like this, to encrypt the file user must provide two input secret keys. First key is up to four-digit secret key and the second key is a single digit secret key. First input key will be reversed for a security purpose then the file (text, image or video) will be decoded into series array of secret bytes then logic operational technique is used to merge array of secret bytes values and the first secret key value and write them back into the file.

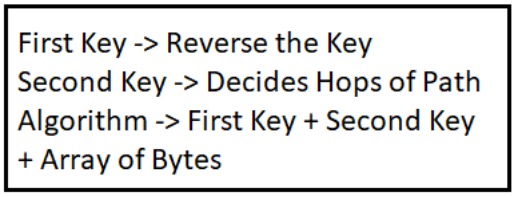


Figure 5.2 – Representation of methods

Based on the second secret key value, a buffer space is created to store the location of path. ACO algorithm technique is used to decide on how long the encryption technique must travel and how many hops it has to travel. At each hop on the distance travelled, the encryption will be repeated. The distance of the travel is based on the second secret key value.

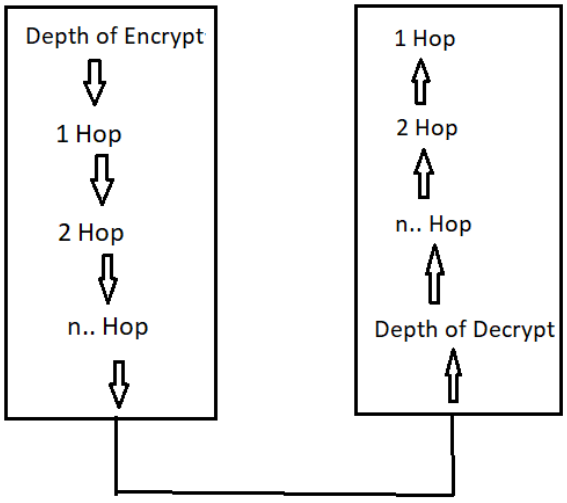


Figure 5.3 – Flow of hops

At each encryption stop, first secret key is turned to another secret key using logic operation technique. It generates the new set of series of array of bytes by combining previous hop values and write them into the file. This entire process is repeated at each hop until it reaches final stage. This unique design makes the encryption key even stronger. Buffer information are merged with the array of secret of bytes and written into the file so that it is carried away and helps during decryption process.

Once the algorithm reaches the final hop, final stage of encryption takes place as explained above and intimate the user. Here the file is completely encrypted. This acts as a double protection as multiple encryptions technique applied to the file. At this stage, File is encrypted completely, and the user is safe to transfer the file as needed.

Once the receiver receives the file, user can decrypt the file. Secret Key or Symmetric key cryptographic method is used here. A user must remember both the secret keys to be able to decrypt the file. When the user enters both the secret codes, the process of decrypting the file starts. Algorithm is intelligent enough to know encrypted file is a ciphertext or visual. Accordingly, it starts the decryption. Remember, here the file contains series of array of secret bytes as it was encrypted at last step.

ACO algorithm plays an important role in decryption process as it helps in optimizing the short distance travelled due to markers left in path during encryption technique. Ant algorithm guides the travel path until reaches the final hop. At each decryption hop, first secret key will be changed to a previous older value using logic operation technique. This is needed to bring back the original first secret key to do a successful decryption at final hop.

At each level of decryption hop, the file will be decoded into series of array of secret byte values, next the first secret key to be reverted then logic operational technique merges array of secret byte values and the reverted first secret key and write them back into the file.

As the distance of the travel is based on the second secret key. Ant algorithm helps the decrypt process to

travel the right and short path until it reaches the final hop. Buffer space information helps the ant algorithm to know the location of path. At each hop, the entire process is repeated to bring back the file to its original stage. Once the path is back to starting point. At this level, User is authorized to view the content which means the decryption process is completed successfully.

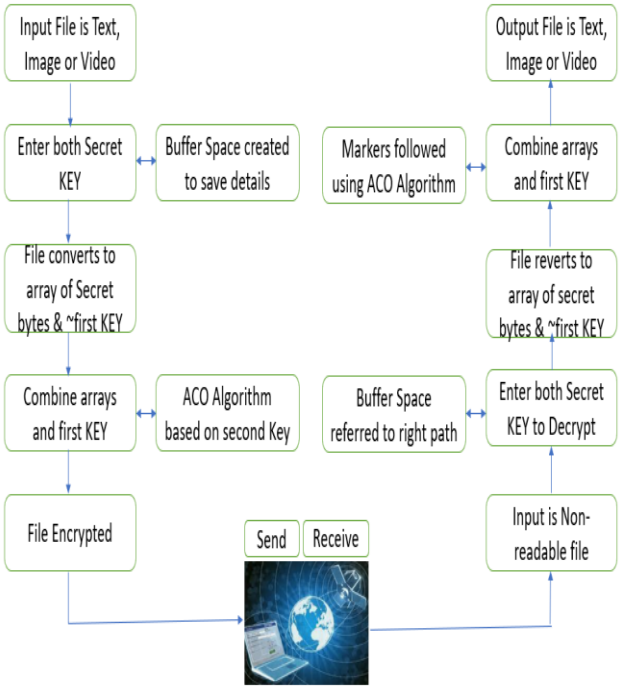


Figure 5.4 – Flow Chart of algorithm

VI. Text, Image & Video sample Results

CIPHERTEXT

INPUT IS .TXT FILE → ENCRYPTION → DECRYPTION → OUTPUT IS .TXT FILE

Figure 6.1 – TXT encrypt/decrypt output

IMAGES

INPUT .GIF IMAGE → ENCRYPTION → DECRYPTION → OUTPUT .GIF IMAGE

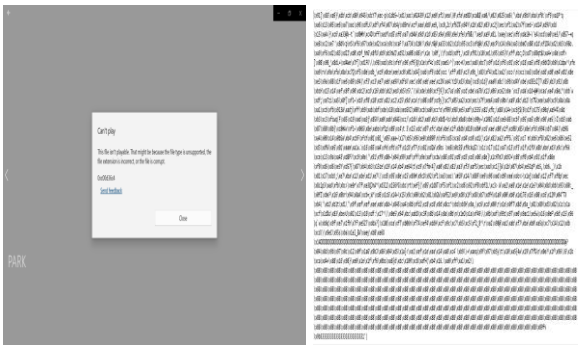
Figure 6.2 – GIF encrypt/decrypt output

ORIGINAL .JPG IMAGE → ENCRYPTION → DECRYPTION → ORIGINAL .JPG IMAGE

Figure 6.3 – JPG encrypt/decrypt output

VIDEOS

INPUT .MP4 VIDEO → ENCRYPTION → UNREADABLE VIDEO FORMAT → DECRYPTION → OUTPUT .MP4 VIDEO



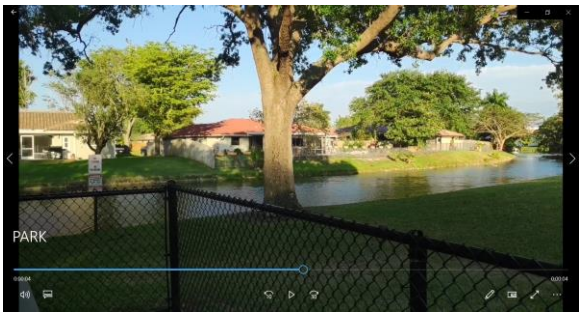


Figure 6.4 – MP4 encrypt/decrypt output

VII. COMPARSION TABLE

Type of File (Texts/Img/ Videos)	File Name	Size of File	Buffer Space	Degree of 2nd KEY	Encrypt Time	Decrypt Time
Text	Accuracy.pdf	1.02 MB	1	Low	774 ms	761 ms
	Accuracy.pdf	1.02 MB	4	Medium	3.3 secs	3.2 secs
Text	Info.txt	4 KB	3	Medium	27 ms	24 ms
	Info.txt	4 KB	7	High	25 ms	24 ms
Image	GC.gif	923 KB	2	Low	1.35 secs	1.23 secs
	GC.gif	923 KB	8	High	3.96 secs	3.48 secs
Image	mahal.jpg	171 KB	5	Medium	532 ms	441 ms
	mahal.jpg	171 KB	2	Low	308 ms	307 ms
Image	Pan.png	94 KB	2	Low	219 ms	213 ms
	Pan.png	94 KB	3	Medium	316 ms	302 ms
	Pan.png	94 KB	7	High	401 ms	420 ms
Image	Egg.jpg	4.07 MB	1	Low	5.1 secs	5.0 secs
	Egg.jpg	4.07 MB	5	Medium	16.8 secs	15.91 secs
	Egg.jpg	4.07 MB	8	High	26.6 secs	26.2 secs
Image	Sand.jpg	6.90 MB	6	Medium	56.12 secs	43.48 secs
	Sand.jpg	6.90 MB	7	High	57.26 secs	1 min 1 sec
Video	vid.mp4	193 KB	1	Low	342 ms	254 ms
	vid.mp4	193 KB	4	Medium	455 ms	434 ms
	vid.mp4	193 KB	7	High	683 ms	553 ms
Video	park.mp4	23 MB	2	Low	117 secs	108 secs
	park.mp4	23 MB	7	High	313 secs	248 secs

Figure 7.1 - Table Comparison output

VIII. TABLE DISCUSSION

50+ different files of texts/images/videos with various sizes have been part of analysis & comparison and the sample results are given in the Fig: table 7.1. The analysis is done based on the different sizes and type of file of texts/images/videos, buffer spaces and second secret key level of degree.

From the analysis it has been found 90% of the scenario, time taken for the decryption is faster than the time taken for the encryption. This shows while decrypt, ACO algorithm is efficiently used to find the shortest path. Also understand, there are several other factors that consume time like OS processes, CPU, Memory, load on system, etc.

IX. CONCLUSION

This research paper shows the uniquely designed algorithm to secure the data at our device itself before we send through internet services. Two key secret code authentication makes it hard for third party to decrypt the file. Incorrect key corrupts the file, so have a copy of file to retry. The ACO algorithm technique helps the decryption faster through markers saved in buffer space. Result comparison table shows how efficiently ACO algorithm technique is used to travel the short distance.

Combination of these multiple techniques in this algorithm make sure the data in file is safe and protect. The users shall be stress free to send the file across internet.

I would further continue my research to improve the large size files on concurrent method to reduce run time. Also increase the second key authentication values that improves security even high. These improvements would make this unique cryptography algorithm method to high security and stronger to hack.

X. REFERENCES

1. Ant algorithm for grid scheduling problem - IPP – BAS, Acad. G. Bonchev, bl.25A, by Stefka Fidanova & Mariya Durchova
2. Research on Various Cryptography Techniques - Yahia Alemami, Mohamad Afendee Mohamed, Saleh Atiewi
3. Wayner, P. : Disappearing Cryptography, Morgan Kaufmann
4. Copyright protection scheme for color images using extended visual cryptography by Sonal Kukreja, Geeta Kasana, Singara Singh Kasana
5. A new Cryptographic Algorithm AEDS (Advanced Encryption and Decryption Standard) for data security - Ali Mohammed Ali Argabi, Md Imran Alam - IARJSET - Vol. 6, Issue 10, October 2019