CRYPTO YOUR BELONGINGS BY TWO PIN AUTHENTICATION USING ANT ALGORITHM BASED TECHNIQUE

Janaki Raman Palaniappan

Brunswick Corporation, USA

ABSTRACT

Everyone realize data is one of the important strategic for any company to run and win the business. Let it be a mobile apps, websites and so on, there are more chances that our personal data like images, videos, texts get expose while we share across for different purposes. Even though the company says app, website forms are encrypted, the said company itself uses the data internally for their business development. This research presents how one can secure own's data themselves before sending. There are many cryptography methods that has evolved from time to time. Upon researching and analyzing, I present a unique method to encrypt and decrypt the data, using combination of techniques such as Cryptographic technique, ANT Algorithm based formula and logic gates that would provide stronger protection to the data. Secure your images, videos with a 2-pin authentication and protection to encrypt and decrypt the data. A user must provide 2 different symmetric pins to encrypt and decrypt, where first pin shall be up to 4-digit secret pin and a second pin is a single digit pin. Single digit pin acts on how many stages the encryption takes place. The proposed method had been experimented on several images and videos. This study reveals, A combination of secret keys, ANT algorithm and Logic gates makes difficult for anyone to hack the data. This unique methodology helps us to protect our data more safely at source device itself.

KEYWORDS

Visual Cryptography, Ant Algorithm, Logic Gates Technique.

1. INTRODUCTION

In the history we know every time one or other emperors were ruling around the world. Now that we live in a computer era where only emperor named 'Internet' is ruling all over the world and entered our personal space. Data in one part of the world is accessible in other part of the world in a millisecond. In the present communication the major issue with data transfer is the security and authenticity.

On a day-to-day basis, we use mobile apps, public email services, websites for different purpose to store/share Images such as Driving License, Passport, Marksheets, etc., and videos that contains sensitive information are very crucial and must be secured. These data are used by companies directly or indirectly to build their business. Unauthorized user hacking this sensitive information could lead to lot of social problems. So, protecting self-data is our own responsibility rather than to be a victim.

David C. Wyld et al. (Eds): ICAIT, CBIoT, WiMo, CRYPIS, ICDIPV, CAIML, NLCA - 2022
pp. 127-133, 2022. CS & IT - CSCP 2022 DOI: 10.5121/csit.2022.121210

My research objective is how one can protect owns data in source itself before we share across. Even though there are many cryptography methods available and evolved, I researched to develop a unique method to encrypt and decrypt the data. This method is a combination of visual cryptographic technique with 2 pin authentication, ant algorithm formula and logic gates technique. This makes a cryptography method unique to encrypt and decrypt the data, making it difficult for anyone to hack the data. This also ensures the data is safe at user end itself.

2. VISUAL CRYPTOGRAPHY

Cryptography is the way to keep the information secret and safe. It helps in hiding the data and allows only intended users to view the content. Cryptography is widely used due to great security. There are 2 methods that are used widely,

Symmetric Key – Both the sender and receiver should have the same key to view the information. Other name for this method is known as Secret Key cryptography.

Asymmetric Key – This cryptography uses pair key based technique i.e., public key and private key to Encrypt and Decrypt the data. It is also named as public key cryptography.

Similarly Visual Cryptography is a technique that allows the images, videos, etc., to be encrypted thatconverts in a non-readable format. Only authorized user is allowed to decrypt the data. Once decrypt takes place, the visual appears the same.

3. ANT ALGORITHM

Ant algorithm is based on the behavior of how ant's searches the food. Ant starts searches, by wander randomly. Once the ant finds the food, it picks and goes back to source place leaving the markers to show the path has food. When other ants come across the markers, they certainly follow the markers and leave their markers thus making the path stronger and shorter.

4. ANALYSIS AND RESEARCH

4.1. Problem

Daily, we use many apps in mobile, public emails, browsers, etc., We share our personal data like photos, Driving License, passport, ids, etc., for different purposes like jobs, verifications, security, etc., Upon sending, our personal data are used by companies for their business development strategy because data analytics/science is one of main key to success and growth. Securing one's own personal data lies in own hand.

Even though there are multiple cryptographic techniques available. I have come up with a unique method of visual cryptography to safeguard the data in our source device itself like mobile, laptop, etc., before we send across internet.

4.2. Method

There are many methods how visual cryptography technique can be used to secure the image. In my experience I decided to take a different path to handle this technique and would like to share my research work.

Encryption using combination of multiple techniques such as 2 PIN authentication, ANT algorithm technique and logic gates technique on how the data to be encrypted. This technique provides a very high security to the data. If anyone wants to view the data, person must decode 2 secret PIN/Code. Combination of 2 secret PINs makes it more difficult for anyone to hack it.

The user who wants to encrypt the image must provide 2 secret codes (Pin1 and Pin2) and remember it. First code (Pin1) is up to 4-digit secret code and the second code (Pin2) is a single digit secret code up to 5. Initially the image will be decoded into series array of bytes, next the first secret code will be inverted to hide original code, then logic gate technique is used to combine array of bytes values and the inverted first secret code value and write them as series of bytes back into the image. At this stage, the image is encrypted partially.

```
Image →Array [ xef, xf4pzkK, x80, ... ]
```

```
key = ~Pin1
Combine = Arrays | ~Pin1
```

Based on the second secret code value, the Ant algorithm technique is used to decide on how long the encryption technique must travel. Also, how long the travel is, the encryption will be repeated at each stage. The length of the travel is based on the second secret code value.

```
Path1 → Path2 → .. PathN
```

At each encryption hop (stage), first secret code will be changed to a different value using logic gate technique. Also generates the new series of array of bytes by combining previous stage series of array of bytes and new inverted first secret code and write them into the image. This process is repeated at each stage until it reaches final stage. This design makes the encryption key even stronger.

Once the ant reaches the final hop which is decided based on second secret code value, final time the encryption technique will be done, and the message is issued to the user. Here the image is completely encrypted. This acts as a double protection and multiple encryptions technique applied to the image.

At this stage, the user is safe to transfer the image to someone or save in an email, etc. It is encrypted.

Once the destination user receives the image, user can decrypt the image. As the symmetric key method is followed here. A user must remember both the secret codes to be able to decrypt the message.

When the user enters both the secret codes, the technique of decrypting the image starts. Remember, here the image contains series of array of bytes as it was encrypted at last step.

Ant algorithm plays a major role in decryption technique as it helps the decrypt hops to follow the travel path (markers) of encryption technique. At each decryption stage, first secret code will be changed to a different value using logic gate technique. Ant algorithm shows the travel path until reaches the final stage.It helps in optimizing the path.

At each decryption hop (stage), again the image will be decoded into series of array of bytes values, next the first secret code to be inverted once again to be able to obtain the hidden original secret code, then logic gate technique is used to combine array of bytes values and the inverted first secret code value and write them as series of bytes back into the image. At this stage, the image is decrypted partially.

Path1 ← Path2 ← .. PathN

As you know the length of the travel is based on the second secret code value. Ant algorithm helps the decrypt technique to travel the right path until it reaches the source. At each decrypting stage, the Ant algorithm technique is used to decide on how long the decryption technique must travel. Also based on the distance of travel, the decryption will be repeated at each stage.

Once the path is back to starting point. At this stage, User is authorized to view the content. Refer Figure4.2.1 for chart representation.

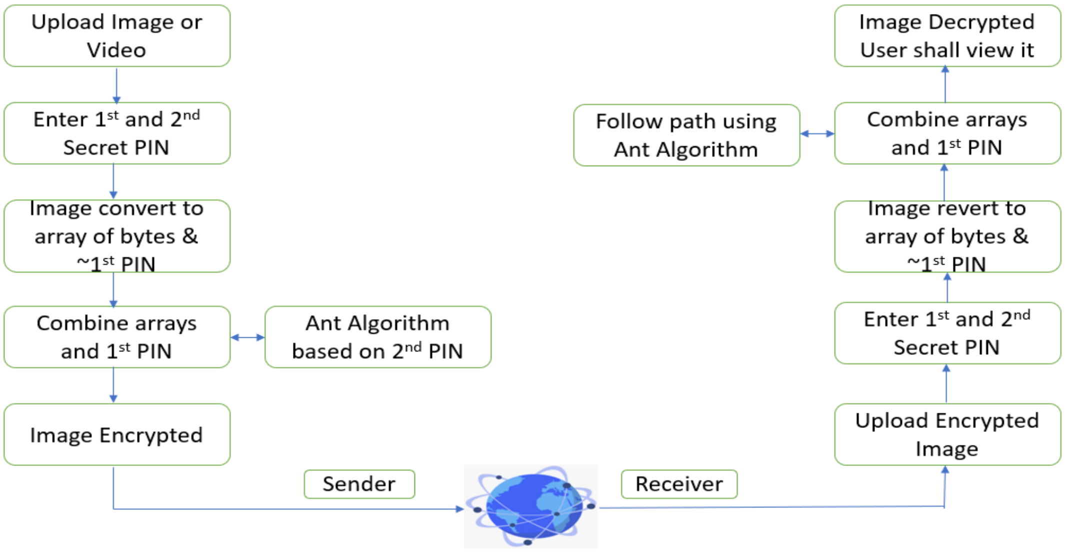

Upload Image or Video
Enter 1st and 2nd Secret PIN
Image convert to array of bytes & ~1st PIN
Combine arrays and 1st PIN
Ant Algorithm based on 2nd PIN
Image Encrypted
Sender
Receiver
Upload Encrypted Image
Enter 1st and 2nd Secret PIN
Image revert to array of bytes & ~1st PIN
Combine arrays and 1st PIN
Follow path using Ant Algorithm
Image Decrypted User shall view it

Figure 4.2.1 – Flow Chart of visual cryptography

The Limitations are,

- When the secret codes PIN are entered wrong the image or video gets corrupted. If user do not remember secret PIN, it is suggested to have a copy of the image or video to retry if PIN are remembered.
- Encryption/Decryption size of the images/videos that were tested are up to 10 MB.
- The 2nd secret PIN was tried with maximum number 5.

4.3. Sample Results

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

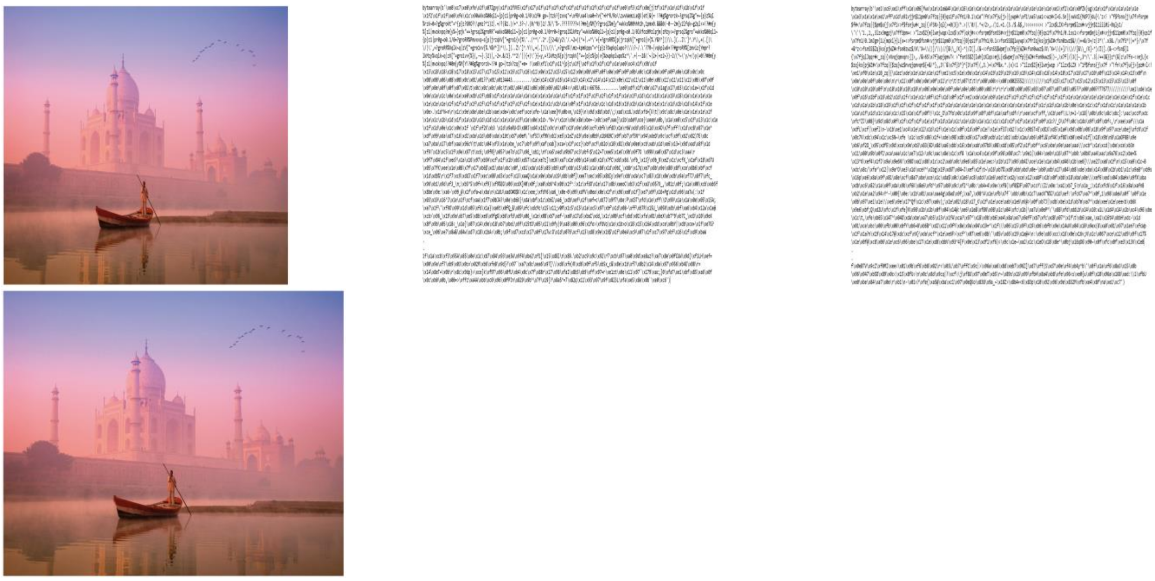


Figure 4.3.1 –JPG encrypt/decrypt output

ORIGINAL .PNG IMAGE → ENCRYPTION →DECRYPTION → ORIGINAL .PNG IMAGE

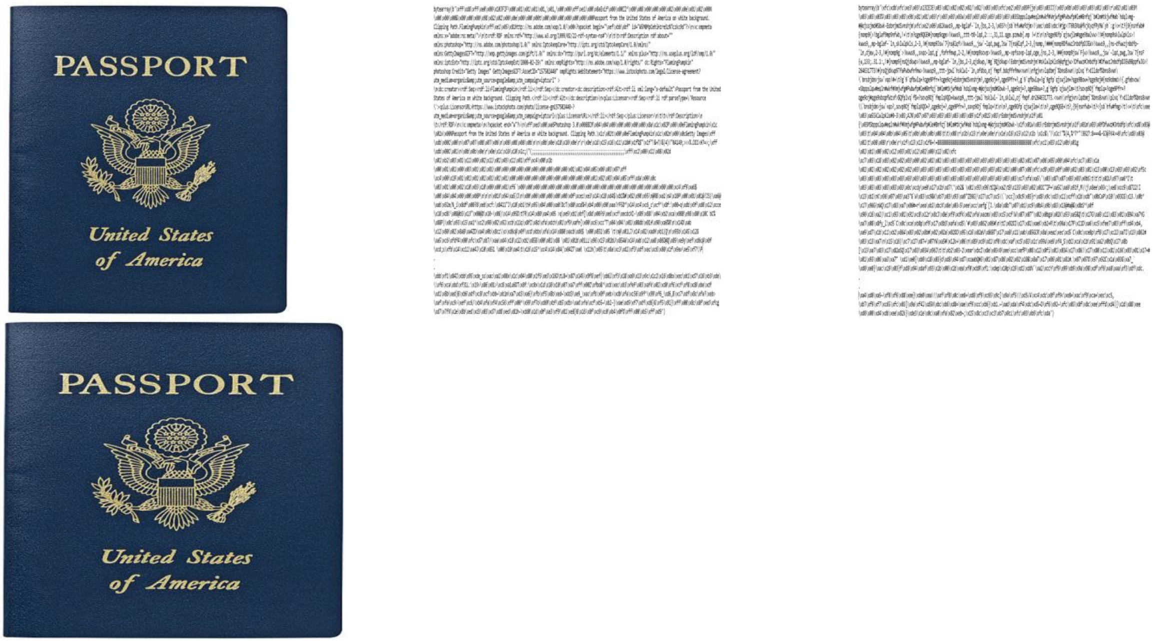
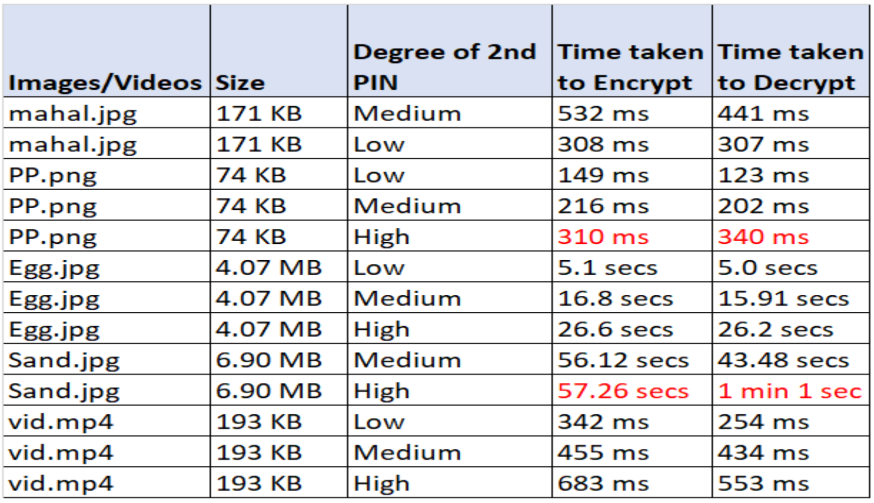


Figure 4.3.2 – PNG encrypt/decrypt output

4.4. Result Comparison



Images/Videos	Size	Degree of 2nd PIN	Time taken to Encrypt	Time taken to Decrypt
mahal.jpg	171 KB	Medium	532 ms	441 ms
mahal.jpg	171 KB	Low	308 ms	307 ms
PP.png	74 KB	Low	149 ms	123 ms
PP.png	74 KB	Medium	216 ms	202 ms
PP.png	74 KB	High	310 ms	340 ms
Egg.jpg	4.07 MB	Low	5.1 secs	5.0 secs
Egg.jpg	4.07 MB	Medium	16.8 secs	15.91 secs
Egg.jpg	4.07 MB	High	26.6 secs	26.2 secs
Sand.jpg	6.90 MB	Medium	56.12 secs	43.48 secs
Sand.jpg	6.90 MB	High	57.26 secs	1 min 1 sec
vid.mp4	193 KB	Low	342 ms	254 ms
vid.mp4	193 KB	Medium	455 ms	434 ms
vid.mp4	193 KB	High	683 ms	553 ms

Figure 4.4.1 – Table Comparison output

4.5. Tabulation Discussion for Ant Algorithm

50+ variety of images/videos with the different sizes have been analyzed and the part of results are given in the Fig: 4.4.1. The analysis is done based on the size of the image/videos and the 2nd secret PIN level of degree.

Based on the 2nd Secret PIN entered, logic gate technique combination of array of bytes values and the inverted first secret code value happens and written them as series of bytes back into the image and it is repeated at each stage.

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, ANT algorithm is efficiently used to find the path. Based on the 2nd pin value, the encryption and decryption time taken varies for the same image. Also understand, there are several other factors that consume time like CPU, Memory, system load, etc.

5. Conclusion

The entire research shows the unique way of securing the data at source itself before we share across. 2 PIN secret code authentication makes it hard for any hacker to decrypt the image. Wrong PIN corrupts data, so better to have a copy to retry. The ANT algorithm technique helps the decryption faster. Result comparison table shows how efficiently ANT algorithm technique is used.

Combination of these multiple techniques makes sure the data is safe and that reduces user stress and shall concentrate on other responsibilities.

My future scope is to increase the 2nd PIN digits values which would make this unique visual cryptography method even stronger. Even the images and videos with higher sizes would be considered for encryption and decryption. My research and contribution would continue towards future scope.

REFERENCES

[1] Ant algorithm for grid scheduling problem - IPP – BAS, Acad. G. Bonchev, bl.25A, by Stefka Fidanova & Mariya Durchova

[2] Wayner, P. : Disappearing Cryptography, Morgan Kaufmann Publisher, 2002

[3] Copyright protection scheme for color images using extended visual cryptography by Sonal Kukreja, Geeta Kasana, Singara Singh Kasana