AmiEs-2023

Enhancing Copyright Protection with AES Encryption and Steganography a Comprehensive Approach for E-Books

Manos Vasilakis[1], Konstantinos Karampidis[1], Manolis Tampouratzis[1], Athanasios Malamos[1], Spyros Panagiwtakis[1]

[1]Department of Electrical and Computer Engineering (ECE), Hellenic Mediterranean University (HMU)

Heraklion, GR 71004 Greece

(mvasilakis@hmu.gr, karampidis@hmu.gr, tampouratzis@hmu.gr, amalamos@hmu.gr, spanag@hmu.gr)

International Symposium on
Ambient Intelligence and Embedded Systems

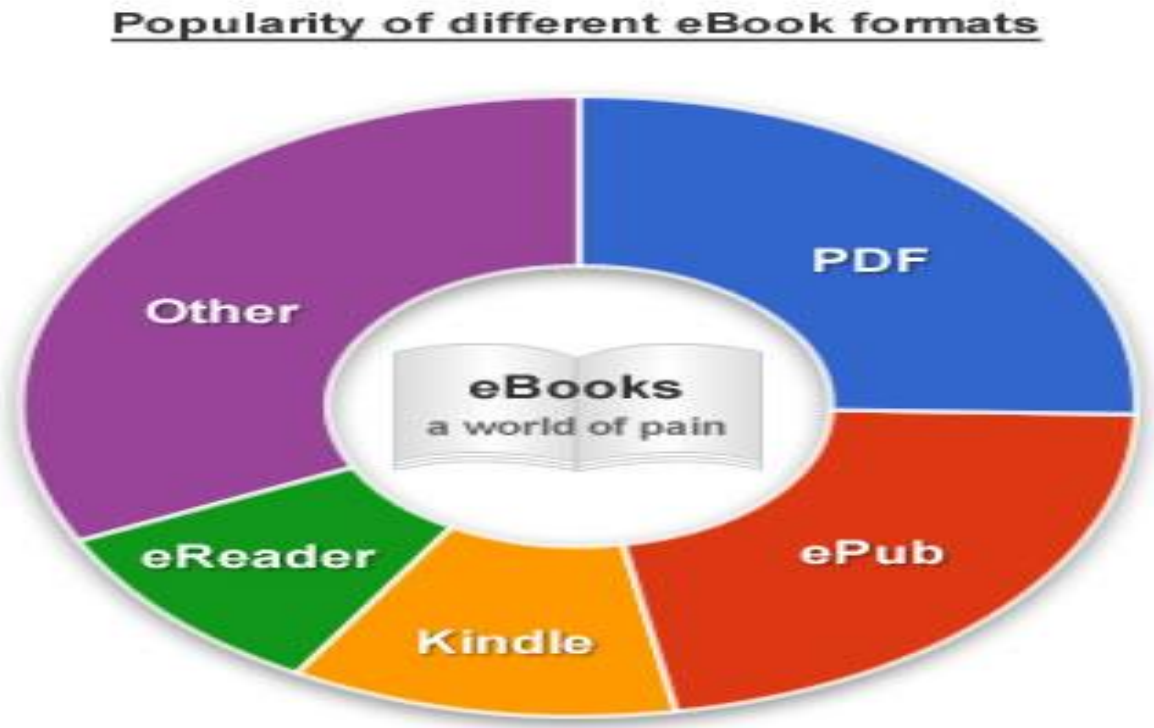
27 - 30 September, 2023
Sitia, Crete, Greece

What was the idea?

• In this study, a web application copyright protection system on e-books Portal Document format (pdf) has been developed, based on some algorithms, including cryptography and steganography to protect copyrights.

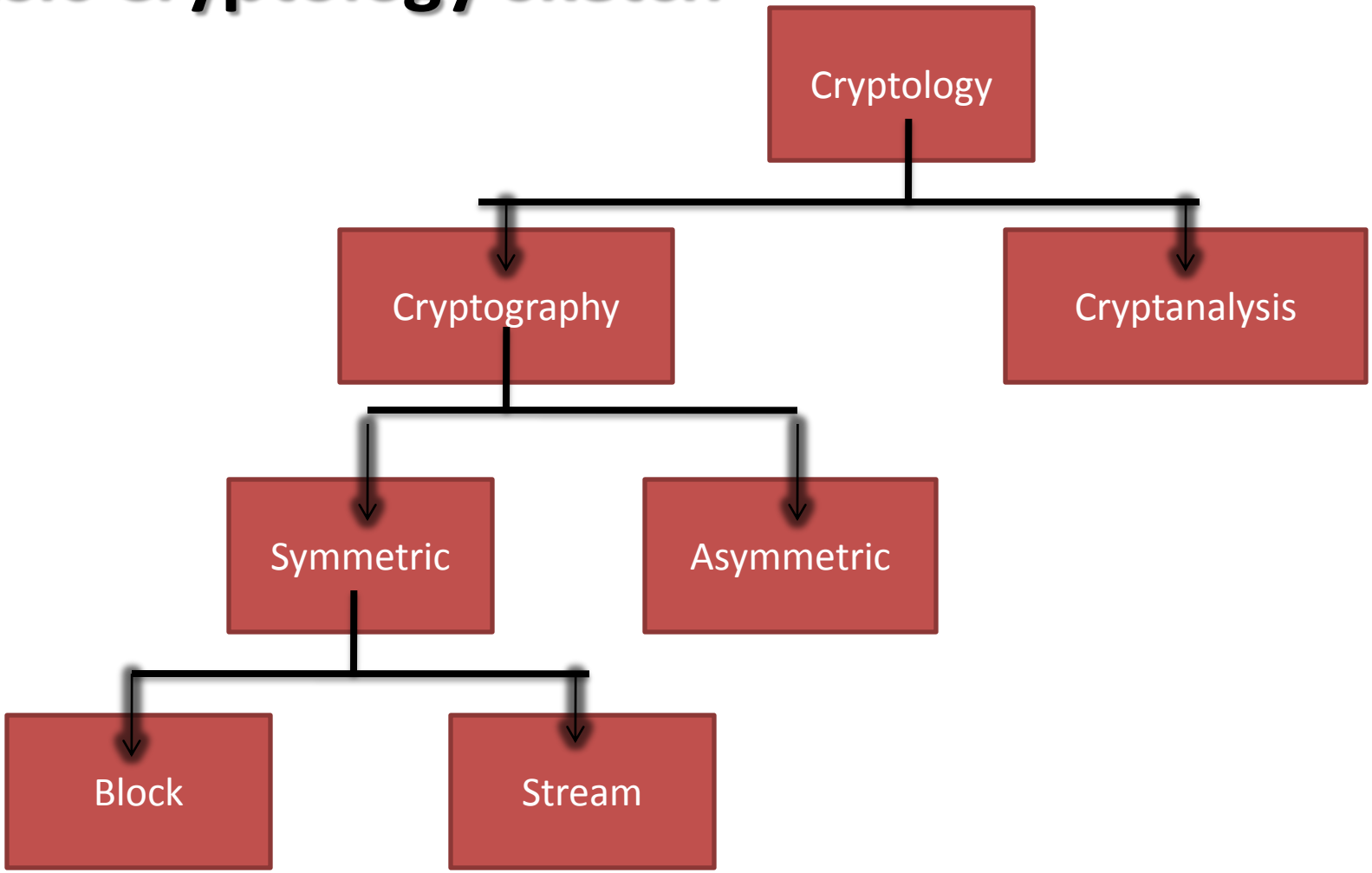
• Thus, enabling users to verify the original buyer of a book, allowing them to identify who purchased the book and who did not. The proposed method could identify the original customer if a PDF is purchased for permanent possession and verified as a buyer by another user.

E-books popularity



E-book file formats(link)

Basic Cryptology sketch



Important expressions on cryptography

Plain text

The plain text called the initial message with information, we want to encrypt it to send the information to the next step .

Cipher text

It is a transformed message produced as output by the algorithm encryption. The cipher text is dependent on both the original message and the secret key, different keys produce different ciphers.

Encryption Algorithm

Makes the necessary transformations of the original text to achieve encrypting a message.

Encryption

Called the conversion process of the original text into cipher

Decryption or deciphering

Called the reverse process of encryption, namely the converting the cipher into original text.

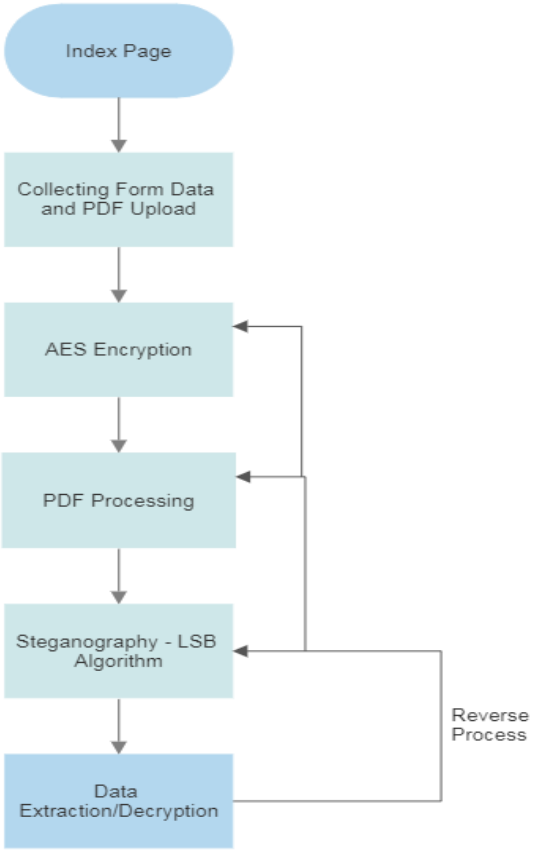
Key

The key is a critical component that is used to transform plaintext data into cipher text.

Padding

Cover a message (padding), call the additional text that should be added to the text so that the original text has real original length requires a cryptographic algorithm. Usually the text is added to the length of the original text followed by zero, obviously cover is removed during decryption.

Overview of Methodology

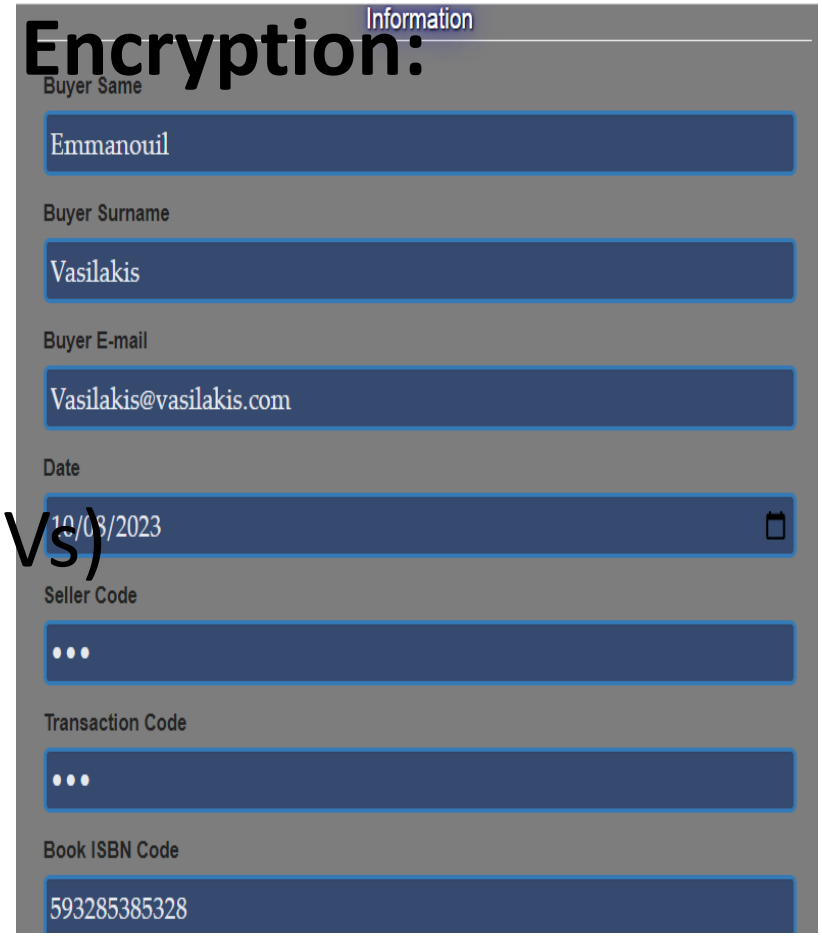


- This methodology combines two powerful techniques. **Cryptography** and **steganography**, to enhance data security.
- By encrypting data using **Advanced Encryption Standard** (**AES)** algorithm and hiding it within images using ***Least Significant Bit*** (**LSB)** steganography, Have been achieved a multi-layered security approach.

Methodology Steps

Step 1 - Data Collection and Encryption:

- Collect user data
- Encrypt it using AES
- Use initialization vectors (IVs) for added more security.



Step 2 – Cover Page Creation

- Create a cover page containing a cryptographic string that consolidates encrypted data segments from the form.
- Encrypt the cover page using AES to ensure that the hidden information remains confidential.

Buyer's Info

Name: Emmanouil

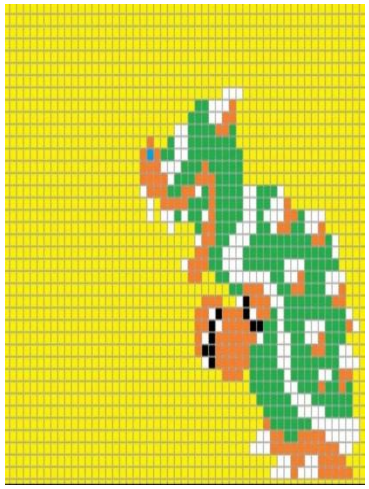
Surname: Vasilakis

j1tBqQkn2s5wE+azR641iM33bafkfOQtz3qa+t6Tps2KRR0oKMmRaCfdDVEdx11kz2bqTgWEphXp
aDtGMAvHqJ0bNacmLLleNtUzU8OF70Y=

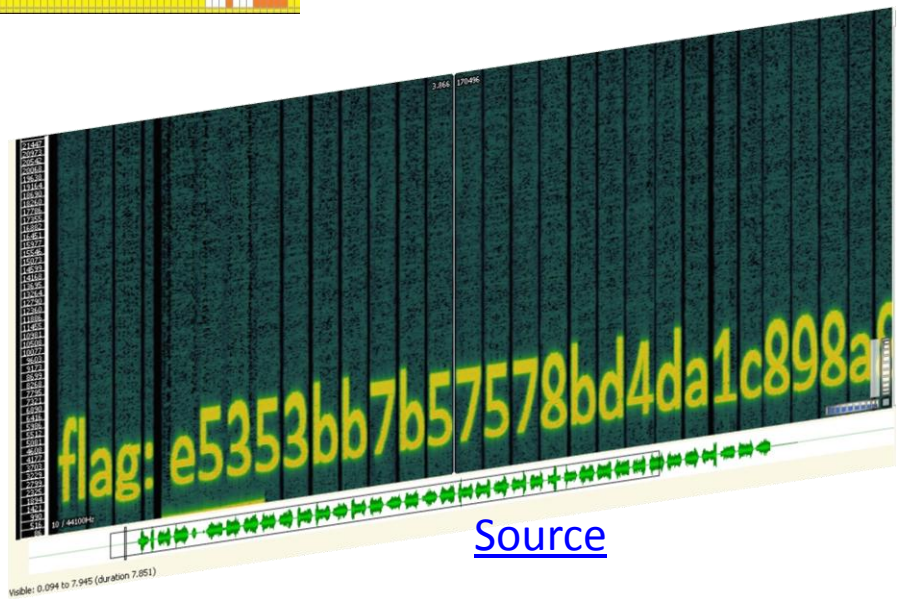
AES – Encryption Algorithm

- The cornerstone of our approach is AES, a cryptographic standard known for its strength and reliability.
- AES encryption transforms plaintext e-book content into cipher text, rendering it unreadable without the decryption key.
- This ensures that the sensitive intellectual property remains confidential, guarding against unauthorized access.

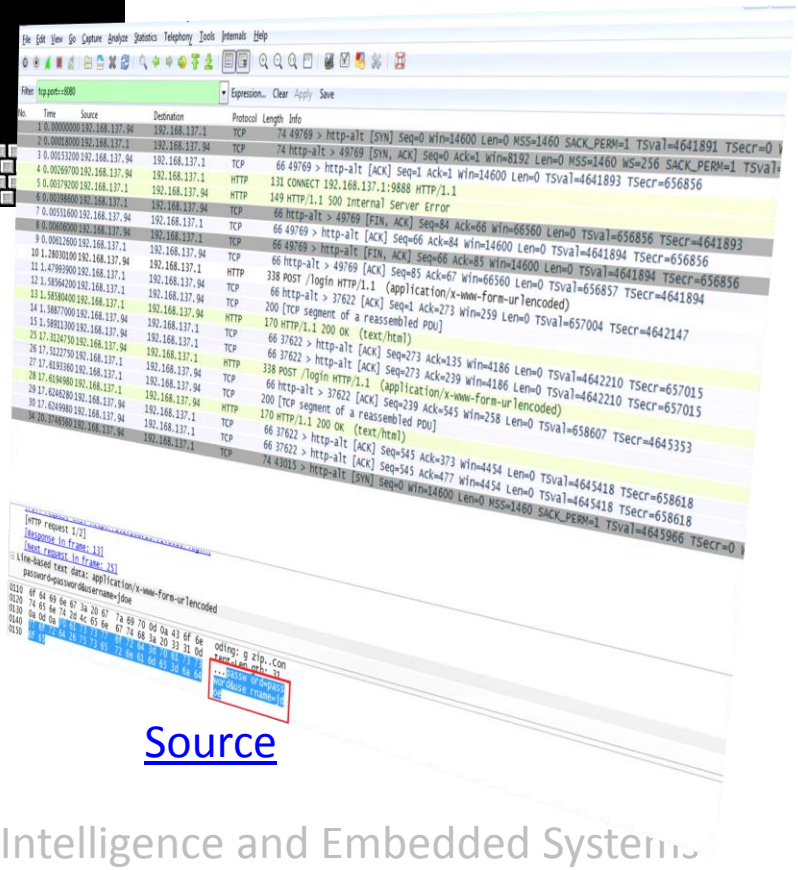
Steganography



Source



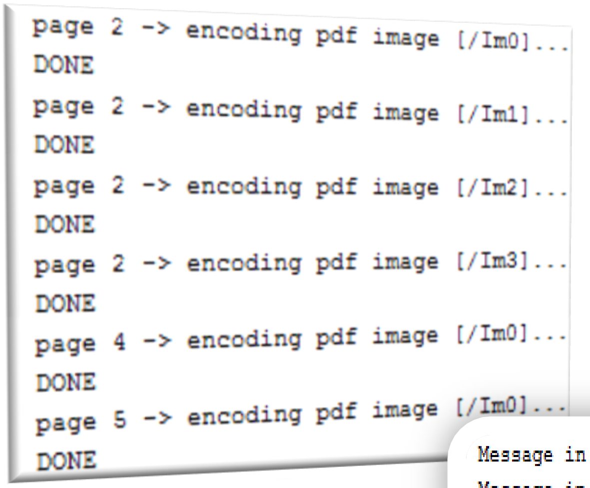
Source

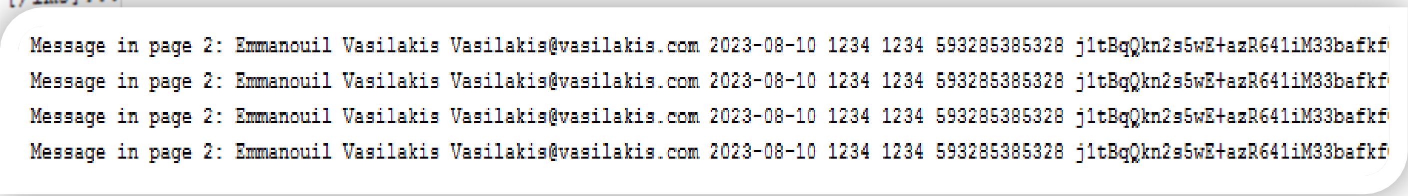


Source

Step 3 - LSB Steganography – Modified Images

Use the LSB steganography algorithm to replace the original images in the PDF with the modified images containing the hidden encrypted data without significantly affecting their appearance.





LSB example

For example, An image with resolution 1024 X 768 pixels the result is:

(1024 X 768 X 3bytes) = 2.359.296 bytes

Suppose we have 3 pixels of an 24 bit image in bytes such as below

00110010	00111001	00110101
00111001	00110010	00111001
00110101	00110010	00111001

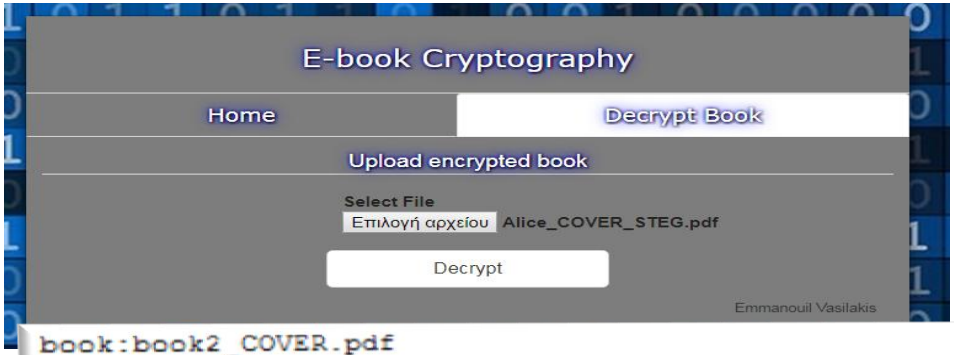
In text is: 295929529

And we can store the byte **011 110 00**, then the original bytes will be changed as follows:

00110010	00111001	00110101
00111001	00110011	00111000
00110100	00110010	00111001

The bits that changed with the original bits are those that have became red. Only 3 bits have changed, without need to change everything bit.

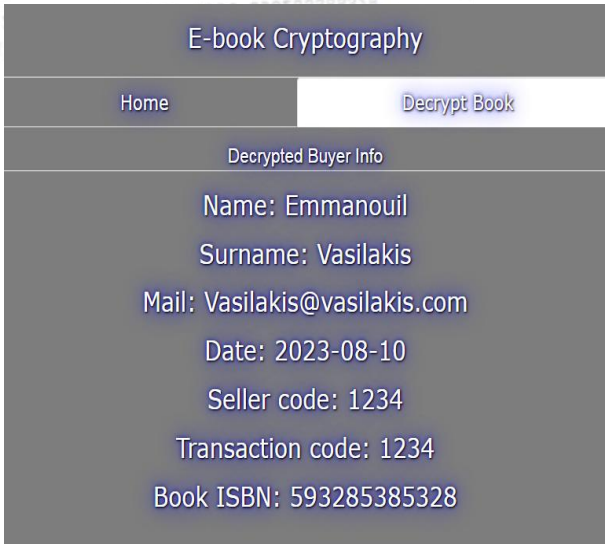
Decryption Process




```
book:book2_COVER.pdf
encIV:Etb0O/0AboOLcjUZNA83eg==
encKey:1GutGtziOTQFvQhOOMo6jw==
line:j1tBqQkn2s5wE+azR641iM33bafkfOQtz3qa+t6Tps2KRR0oKMmRaCfdDVEdx11kz2bqTgWEphXp
line:aDtGMAvHqJ0bNacmLLleNtUzU8OF70Y=
encr:j1tBqQkn2s5wE+azR641iM33bafkfOQtz3qa+t6Tps2KRR0oKMmRaCfdDVEdx11kz2bqTgWEphXpaDtGMAvHqJ0bNacmLLleNtUzU8OF70Y=
Decrypted Information String:Emmanouil Vasilakis Vasilakis@vasilakis.com 2023-08-10 1234 1234 593285385328
```

Data Extraction:

- To extract the data from the modified PDF, reverse the process.
- Extract the LSBs of the image pixels to retrieve the binary representation of the encrypted data.
- Decrypt the encrypted data using the AES decryption algorithm with the appropriate key and IV.



Conclusions

- Our innovative solution redefines copyright protection in the digital age.
- Combining cryptography and steganography provides robust data security.
- The methodology's multi-layered approach strengthens protection against attack vectors.

QUESTIONS?