



Amrita Vishwa Vidyapeetham
Centre for Excellence in Computational Engineering and Networking
Amrita School of Engineering, Coimbatore

AES Enhanced Visual Cryptography Application

GROUP-14 BATCH-B

- 1.POBBATHI SAI SIDDHARTH (CB.EN.U4AIE21146)**
- 2.RAVULAPATI VINAY SAI (CB.EN.U4AIE21153)**
- 3.SANKURABHUKTA SRI MIDHINESH (CB.EN.U4AIE21162)**

Supervised by:

Dr. Sunil Kumar S Asst. Professor

ACKNOWLEDGMENT

We are deeply thankful to **Centre for Excellence in Computational Engineering and Networking (CEN)** at **Amrita Vishwa Vidyapeetham, Coimbatore** for providing us such a wonderful environment to pursue our research. We would like to express our sincere gratitude to **Dr. Sunil Kumar S, Asst. Professor, Department of Centre for Excellence in CEN**, Amrita Vishwa Vidyapeetham. We have completed our research under his guidance. We found the research area, topic, and problem with her suggestions. We would also like to acknowledge our team members for supporting each other and be grateful to our university for providing this opportunity for us. Lastly special thanks to Centre for Excellence in CEN for providing this opportunity to research in this field.

Cryptography

The science of safeguarding communications from outside observers is known as cryptography. Encryption techniques take the original communication (plaintext) and turn it into ciphertext, which is incomprehensible. The key enables the user to decrypt the message, ensuring that it can be read. The strength of an encryption's unpredictability is also investigated, making it more difficult for anyone to determine the algorithm's key or input. To improve our privacy, we can use cryptography to create more secure and robust communications. Advances in cryptography make it more difficult to break encryptions, limiting access to encrypted files, folders, and network connections to authorised users.

The four goals of cryptography are as follows:

- **Confidentiality** ensures that only the intended receiver may decode and read the contents of the message.
- **Non-repudiation** indicates that the sender of the message cannot refute their motives for sending or creating the message in the future.
- **Integrity** refers to the capacity to ensure that the information included in a communication is not altered while it is in storage or transit.
- **Authenticity** ensures that the sender and recipient can authenticate each other's identities as well as the message's destination.

Types Of Cryptography

Symmetric Key Cryptography:

When a secret key is used for both encryption and decryption, it is referred to as symmetric key cryptography or symmetric encryption. This method is the polar opposite of asymmetric encryption, which uses one key to encrypt and another to decrypt data. Data is changed to a format that can't be read or inspected by anyone who doesn't have the secret key used to encrypt it throughout this process. The strength of the random number generator used to generate the secret key determines the success of this strategy. Symmetric key cryptography, which is commonly used on the Internet today, is made up of two types of algorithms: Block and Stream. The Advanced Encryption Standard (AES) and the Data Encryption Standard (DES) are two popular encryption algorithms. This type of encryption is typically faster than asymmetric encryption, but it requires the secret key to be known by both the sender and the recipient of the material.

Hash Functions:

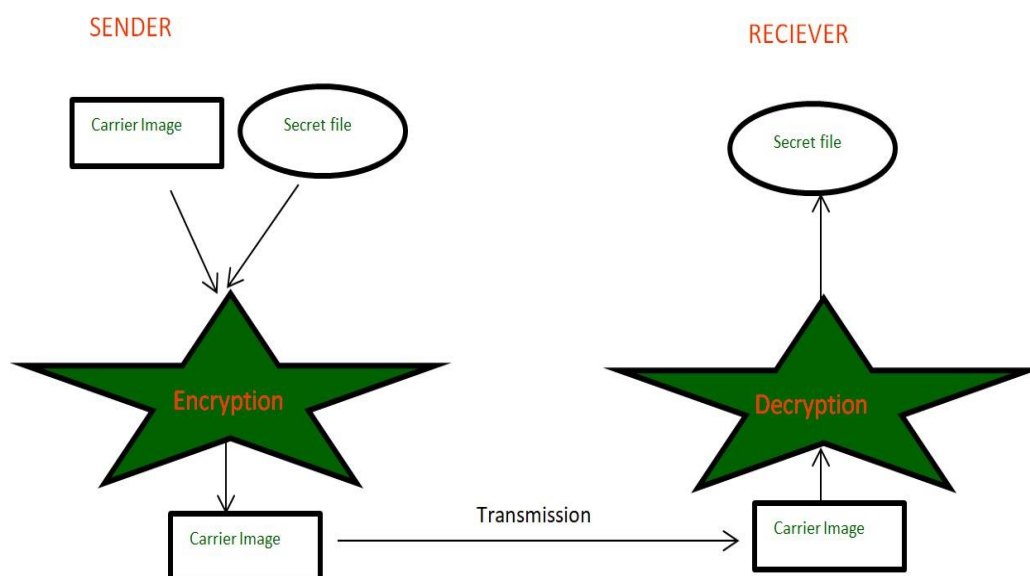
A function that converts a large phone number into a little integer value that can be used. In the hash table, the mapped integer value is utilised as an index. A hash function, in simple words, converts a large number or string into a small integer that can be used as the index in a hash table.

Asymmetric Key Cryptography:

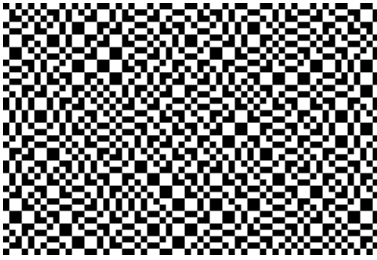
Asymmetric encryption employs two separate but related keys. The Public Key is used to encrypt data, while the Private Key is used to decrypt it. The Private Key is designed to be private, as the name implies, so that only the authenticated receiver can decode the message.

Visual Cryptography

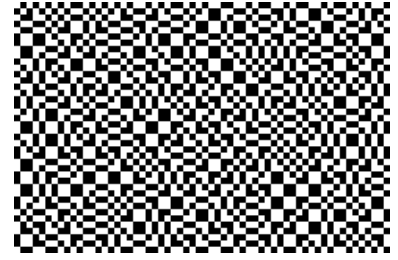
Visual cryptography is a cryptographic approach that encrypts visual data (images, text, etc.) in such a way that it can only be decrypted by sight reading. Visual cryptography, a degree-related emerging encryption technology, rewrites encrypted photographs using human visual features. Visual cryptography allows for safe digital transmission that is only utilised once.



Various types of information, such as military maps and commercial identifications, are distributed via the internet. When creating hidden images, security issues must be considered because hackers can use a weak link in the communication network to steal information. Various image secret sharing techniques have been created to address the security issues with secret photos. Anyone can use it to code with non-science data and perform any computations.



The basis of the technique is the superposition (overlying) of two semi-transparent layers. Imagine two sheets of transparency covered with a seemingly random collection of black pixels



There is no discernible message printed on any of the sheets alone. If the two grids are superimposed perfectly and in the exact precise spot, a message appears! The patterns were created with the intention of revealing a message.

How does it work?

For the source, we start with a monochromatic image. The image's pixels are either white or black. The first example's source can be found to the bottom.

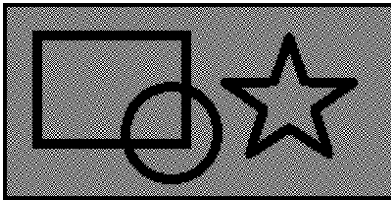


Each pixel is then subdivided into four smaller subpixels. Shade these four subpixels to symbolise the source image, then divide them subjectively between the two cypher images we're making.









































The colour of each pixel in the original source image is examined. We fill in all four sub pixels and distribute them two per cypher layer if the original pixel in the image is set (black). We toss a coin to see which pattern goes on which layer (so that it is random). When all four pixels are combined, it makes no difference which pair of pixels goes on which layer.

If a pixel in the source image is white, we only shade in two pixels. This time, though, we make certain that the same pixels on both layers are shaded. When the two cypher images are joined in this way, just two pixels are darkened. To choose which chiral set to use, we flip a coin again, and make sure the identical image appears on both layers.



As a result of this technique, two images (each two times the size of the original) are created, each with half the contrast of the original. In the combined cypher, the source's black remains black, but the white is altered to a randomly mottled half-tone grey. Fortunately, the contrast is still strong enough for the secret message to be read easily.

Below is the set of rules for Encrypting black and white images for two shares.

pixel												
share1	0	1	2	3	4	5	0	1	2	3	4	5
												
share2												
stack												

Encryption and Decryption using AES and SHA – 256

Hashing Algorithm

A **hashing algorithm** is a mathematical algorithm that converts an input data array of a certain type and arbitrary length to an output bit string of a fixed length. Hashing algorithms take any **input** and convert it to a uniform message by using a **hashing table**.

Background

Hash algorithms were a breakthrough in the cryptographic computing world. This special type of programming function is used to store data of *arbitrary* size to data of a *fixed* size. Hash functions were created to compress data to reduce the amount of memory required for storing large files. The hashes they create can be stored in a special data structure called hash tables, which enables quicker data lookups.

The core reason for hash functions arose from the need to compress content, but the unique identifiers of hash values soon became a staple of simplicity in database management. No two hash inputs should ever return the same hash, but instead create singularly unique identifiers for each hash input. When two different hash inputs return the same output hash, it is called a *collision*.

While hash functions were created to help speed up database upkeep, the utility of hashing algorithms evolved dramatically. A more extensive family of hash functions were created with privacy, security and transparency in mind.

What is a Hashing Function?

Hash functions differ by type; however, there are several characteristics that persist between them.

Deterministic: The hash value remains the same. No matter how many times you input a message into the hashing function you need to receive the same output. The deterministic nature is key to creating order within the system utilizing the hash function.

Quick Computation: For a hash function to be used for real-world applications there needs to be efficient computation for any given message. The hashing function should quickly return a hash value for any potential given message.

Irreversible: There is no reverse engineering; messages cannot be re-traced from the hash output. It is impossible for an input to be regenerated from its hash value. The hash algorithm is designed to be a one-way function so if the hash function can be reversed then it is deemed compromised and no longer viable for storing sensitive data.

Popular Hashing Algorithms

Numerous hashing algorithms have been developed throughout the course of digital forensics, of which some of the most prominent include:

Message Digest 5 (MD5)

No longer actively used, MD5 was one of the most common hashing algorithms in early cryptography. Because of its several vulnerabilities, including the frequency of *collisions*, no cryptocurrencies make use of the 128-bit outputs.

RSA

Named after its designers (Rivest-Shamir-Adleman), RSA is a cryptosystem that originated in the late twentieth century. RSA uses a simple method of distribution: Person A uses Person B's public key to encrypt a message and Person B uses a private key, which remains secret to the user, to uncover its meaning. No active cryptocurrencies use the RSA framework.

Secure Hash Algorithm (SHA)

Secure Hash Algorithm (SHA) is a family of cryptographic hash functions that are used by most cryptocurrencies. This family of cryptographic hash functions were developed by the National Institute of Standards and Technology. Each hashing algorithm released under the SHA family builds upon the last version and since 2000 there has not been a new SHA algorithm released. SHA-384 is used to protect NSA information up to TOP SECRET. Consider this one of the most secure hashing algorithms.

Secure Hash Algorithm (SHA)

SHA algorithm is Secure Hash algorithm that was developed to modify the MD4, in other words, we can say that the SHA algorithm is the modified version of MD4. SHA is designed to obtain the original message, given its message digest, and find the message producing the same message.

What is SHA Algorithm?

In the field of cryptography and crypt analytics, the SHA-1 algorithm is a crypt-formatted hash function that is used to take a smaller input and produces a string that is 160 bits, also known as 20- byte hash value long. The hash value therefore generated, is known as a message digest which is typically rendered and produced as a hexadecimal number which is specifically 40 digits long.

Advanced Encryption Standard (AES)

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

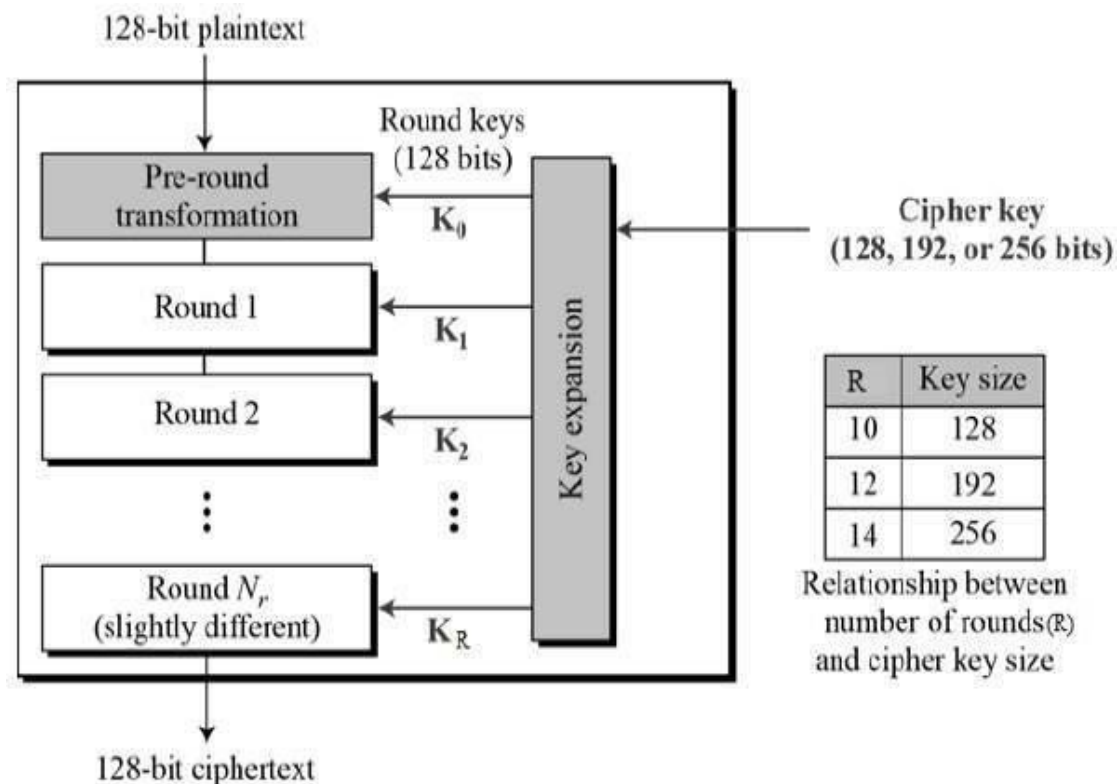
Operation of AES

AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix –

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration –



Linear Regression Process

1. Training the Linear Regression Model:

- The code uses the LinearRegression class from the sklearn.linear_model module to create a linear regression model.
- The model is trained using two sets of data frames (xdf and ydf). These data frames are created by summing up pixel values from different images (P and R) in a specific pattern.
- The purpose of training the linear regression model is to learn a mapping between the pixel sums of the input images (xdf and ydf). This mapping will be used later in the encryption and decryption processes.

2. Prediction Using the Linear Regression Model:

- After training, the code uses the trained linear regression model (LRmodel) to make predictions on a new set of features (zdf).

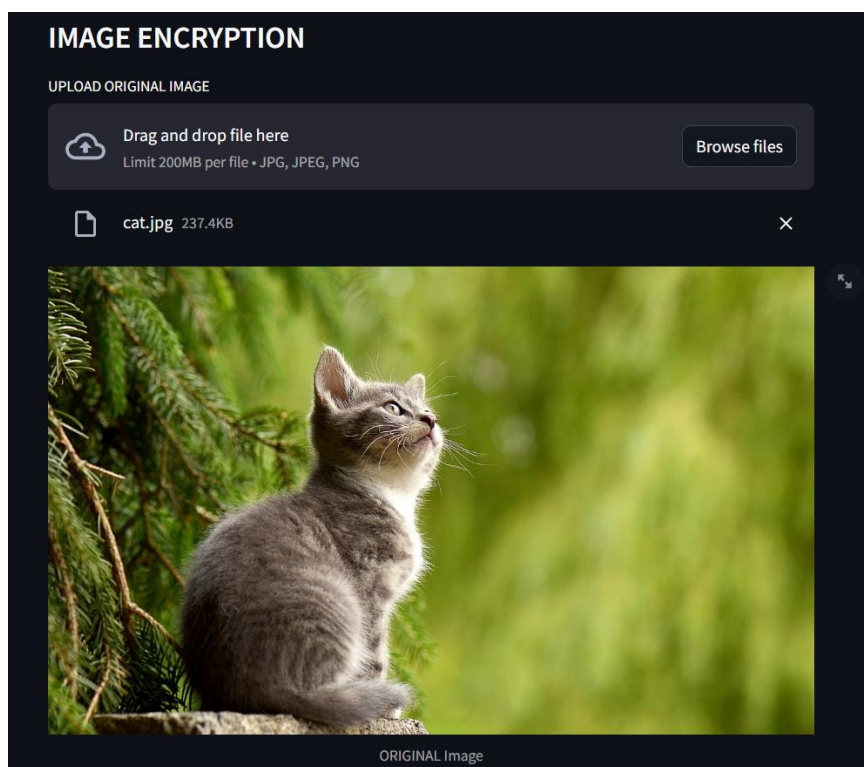
- The features in zdf are derived from a combination of pixel values from the encrypted image (CK), and the model predicts a new set of values.
- These predicted values are then used to determine specific parameters (x and y) required for the encryption and decryption steps.

3. Role in Image Encryption and Decryption:

- The predicted values (x and y) obtained from the linear regression model are used in the encryption and decryption processes.
- These values influence the manipulation of pixel values in the encryption and decryption steps, adding a level of complexity to the process.
- The linear regression model essentially acts as a mathematical tool to determine how the encryption and decryption parameters should be adjusted based on the features extracted from the images.

In summary, linear regression is employed to model the relationship between pixel sums of specific image features, and the trained model is later used in the encryption and decryption steps to determine parameters for manipulating pixel values.

Results



Enter Key:

cryptography

The hexadecimal equivalent of SHA256 is :

e06554818e902b4ba339f066967c000da3fcda4fd7eb4ef89c124fa78bda419

ENCRYPTION



Share 1



Share 2

Decrypt

DECRYPTION



PC

Decrypted Image

Image is Decrypted ...

Future Scope

The Visual Cryptography project has promising future prospects for improvement and expansion. Key areas include enhancing security, supporting more image shares, improving user authentication, refining the user interface, and optimizing performance. These efforts aim to create a more user-friendly and secure experience. Additionally, exploring collaboration features, adapting to quantum computing challenges, and engaging the developer community through open-sourcing contribute to the project's growth and innovation.

References

- 1) https://link.springer.com/chapter/10.1007/978-3-642-14298-7_5
- 2) https://link.springer.com/chapter/10.1007/3-540-44709-1_26
- 3) https://ieeexplore.ieee.org/abstract/document/7732289?casa_token=nh4QBGJbLB8AAAAA:JyvFPRZ57Z_kJYpITjppiX5y6Ex6_8fANnd_uuyU9us9LM76UivmMmr4n3lQO6SL-FLRD7BW9Tjnvw
- 4) <https://www.sciencedirect.com/science/article/pii/S1877050915032445>
- 5) <https://nordvpn.com/blog/sha-256/#:~:text=SHA%2D256%20can%20help%20secure,decrypt%20and%20verify%20the%20signature.>