IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# ENCRYPTION USING AES AND VISUAL CRYPTOGRAPHY THROUGH LSB

[1]Kavya V R, [2]Nisarga S Gowda, [3]Aishwarya P, [4]Nafza A

[1] Assistant Professor, [2] Student, [3] Student, [4] Student

Department of Information Science and Engineering,
Cambridge Institute of Technology, Bangalore, India

***Abstract:*** A novel and highly secure encryption methodology using a combination of AES and visual crypto. With the ever-increasing human dependency on The Internet for performing various activities such as banking, shopping or transferring money, there equally exists a need for safe and secure transactions. This need automatically translates to the requirement of increased network security and better and fast encryption algorithms. This paper addresses the above issue by introducing a novel methodology by utilizing the AES method of encryption and also further enhances the same with the help of visual cryptography. In this method the secret message is divided into two parts after which the message the first half of the message is encrypted using AES and the second share of the message is embedded in the image using LSB.

## I. INTRODUCTION

### 1.1 HIGH SECURITY ENCRYPTION USING AES & VISUAL CRYPTOGRAPHY THROUGH LSB

This paper introduces a novel and highly secure encryption methodology that integrates AES and visual cryptography. In today's increasingly interconnected digital landscape, safeguarding transactions against threats is paramount. This necessitates robust network security and sophisticated encryption protocols. The proposed approach combines AES encryption with visual cryptography, offering a pioneering solution to this challenge. In this method, the secret message undergoes bifurcation: the first half is encrypted using AES, while the second half is embedded in an image using LSB technique.

### 1.2 PURPOSE

Encryption plays a central role in establishing a culture of security and privacy in modern digital environments. Since its designation as the global encryption standard in 2001, AES has significantly outperformed its predecessor, the Data Encryption Standard, addressing many of its shortcomings. It has become the cornerstone of encryption across diverse applications. This project, titled "High Security Encryption Using AES," aims to enhance image security through a fusion of visual cryptography and image compression techniques. Cryptography, the art of securely encoding and decoding information, is instrumental in protecting data from unauthorized access. For this study, secondary data were collected from reputable sources. Monthly stock prices for sample firms were sourced from the KSE website for the period of January 2010 to December 2014. Additionally, macroeconomic data were gathered from the SBP website for a five-year period. The collected time series monthly data encompass stock prices for sample firms and relevant macroeconomic variables spanning from January 2010 to December 2014.

Monthly prices of the KSE-100 Index were sourced from Yahoo Finance

## II. LITERATURE SURVEY

### 2.2.1 Advanced Encryption Standard (AES) Optimization Strategies

In their seminal work, Xinmiao Zhang et al. (2002) introduced a comprehensive exploration of methodologies aimed at optimizing the implementation of the Advanced Encryption Standard (AES) algorithm in hardware. These optimization strategies are broadly categorized into two main classes:

Architectural Optimization: This approach encompasses sophisticated techniques such as pipelining, loop unrolling, and subpipelining. By concurrently processing multiple rounds, architectural optimization endeavors to enhance computational speed. However, this speed enhancement often comes at the expense of increased hardware resource utilization. Notably, within the realm of architectural optimization, loop unrolling exhibits a modest speedup while incurring a notable area overhead.

Conversely, in non-feedback scenarios, sub-pipelining can achieve maximal speedup with an optimal speed-to-area ratio.

### 2.2.2 Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) stands as a cornerstone in modern symmetric block cipher encryption, standardized by the National Institute of Standards and Technology (NIST) under U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. Developed by Joan Daemen and Vincent Rijmen, the Rijndael algorithm serves as the foundation for AES. Comprising two primary units, namely the Data Processing Unit and the Key Expansion Unit, AES operates on 128-bit data blocks utilizing secret keys of varying sizes: 128-bit, 192-bit, or 256-bit, denoted as AES-128, AES-192, or AES-256, respectively.

### 2.2.3 Transformations in AES

Sub Byte Transformation

The SubByte transformation, a pivotal nonlinear function within AES, operates independently on each byte of the state, facilitated by a substitution table known as the S-box. In hardware realization, optimizing the S-box design is imperative. Two fundamental approaches emerge: designing multiplicative inversion and affine transformation separately, or constructing a logic circuit defining the input-output mapping of the S-box function.

A. **Shift Row Transformation**

The ShiftRow transformation, akin to SubByte, operates autonomously on each byte of the state, effecting a rearrangement of byte order within each 128-bit block through cyclic shifts across the last three rows of the state.

B. **Mix Column Transformation**

Rooted in Galois Field multiplication, the MixColumns transformation substitutes each byte of a column with a value derived from all four bytes in the respective column. This transformation, integral to the encryption process, endeavors to obfuscate columnar byte patterns.

C. **Add Round Key and Key Expansion**

The AddRoundKey operation involves applying the round key to the state via a bitwise XOR operation. Meanwhile, the Key Expansion unit is responsible for generating subsequent round keys through iterative processes akin to those employed within the Data Processing Unit.

i. **Add Round Key**

In a departure from other encryption steps, the AddRoundKey operation is applied twice, with the initial application preceding the encryption iterations. This initial round key addition, implemented via a straightforward exclusive-OR operation, integrates the initial key with the data block.

ii. **Key Expansion**

Key expansion orchestrates the derivation of all Round Keys from the initial input key. During encryption, the initial round key mirrors the original key itself. Conversely, during decryption, the initial round key corresponds to the first group of keys generated during key expansion, with the final decryption round utilizing the last group of keys. For a 128-bit key size, the key expansion process yields 10 round key groups, each comprising 16 bytes.

## III. LITREATURE SURVEY OF VISUAL CRYPTOGRAPHY

The first Visual Cryptography Scheme (VCS) was proposed by Naor and Shamir, utilizing whiteness to distinguish between black and white colors. A black-and-white secret image is divided into noise-like shadows by breaking down a secret pixel into m subpixels (referred to as pixel expansion) in each of n shadows. This expansion increases the shadow size by a factor of m, thereby degrading the visual quality of the reconstructed image. Numerous research papers have been published aiming to reduce this pixel expansion. Some achieve no pixel expansion (m = 1). VCSs typically produce noise-like shadows with black and white random dots, making them difficult for identification and management. However, VCSs with meaningful shadows, known as extended VCS (EVCS), have been developed. EVCS takes a secret image and n original share images as inputs, producing n shares meeting three conditions: 1) any qualified subset of shares can recover the secret image; 2) any forbidden subset cannot obtain information beyond the secret image's size; 3) all shares are meaningful images.

Comparisons among different EVCSs reveal unique advantages. For example, the proposed EVCS preserves the most details of share images, Zhou et al.'s EVCS generates the brightest shares, and Wang et al.'s second EVCS produces the smoothest shares. Further comparisons on fine share images show the proposed scheme's superiority, particularly in maintaining share details.Cheating Immune Threshold Visual Secret Sharing schemes address the possibility of dishonest participants compromising the security of the secret. These schemes prevent cheating through various methods, such as using additional shares and a confidential image or employing specific threshold schemes. Color-black-and-white VC studies aim to reduce pixel expansion and enhance reconstructed image quality. These schemes use probabilistic and random grid-based methods to generate non-expansible shares. Naor and Shamir's (k,n)-VCS shares black-and-white secret images into corresponding shadows using Boolean base matrices. CBWEVCS introduces black and white matrices, minimizing pixel expansion compared to conventional VCSs. These schemes ensure perfect black schemes, maintaining contrast and extending capabilities in image reconstruction.

## IV. LEAST SIGNIFICANT BIT

In computing, the least significant bit (LSB) holds the least value and is located farthest to the right in a multi-bit binary number. Binary numbers are fundamental in computing, and the LSB is particularly crucial, especially in binary data transmission.

Binary data is processed and transmitted in binary format, where the rightmost digit is the least significant and the leftmost is the most significant. The LSB is also referred to as the rightmost bit due to its position in positional notation. It contrasts with the most significant bit (MSB), which holds the highest value and is located farthest to the left in a multi-bit binary number. In a multi-bit binary number, the significance of a bit decreases as it moves towards the LSB. The MSB and LSB represent the two extremes in terms of significance within the binary number.

When transmitting binary data using the least significant bit first technique, the LSB is transmitted first, followed by the other bits in increasing order of significance. This technique is commonly used in various applications such as hash functions, checksums, and pseudorandom number generators. In summary, the LSB plays a crucial role in binary representation and transmission, and its significance is essential in various computational tasks and algorithms.

## V. Design

### 4.1 PURPOSE

This chapter provides an overview of the design of the proposed system. It outlines the architecture of the system, starting from conceptual design and elaborating on details added during subsequent design phases. The chapter also discusses the static and dynamic behavior of individual entities within the system. The documentation produced in this chapter influences the implementation and testing phases of the project, with details expected to evolve throughout the design process.

4.2 LEAST SIGNIFICANT BIT

The Least Significant Bit (LSB) technique is a spatial domain method wherein each bit of text or image data is substituted from the least significant bit of the original image. This technique is straightforward and easy to implement. Its effectiveness in the spatial domain stems from the fact that the human eye cannot easily distinguish between the original and encrypted images. The LSB technique can extend up to 4 bits or 2 bits out of 8 bits, but it may introduce distortion in the image due to changes in intensity.

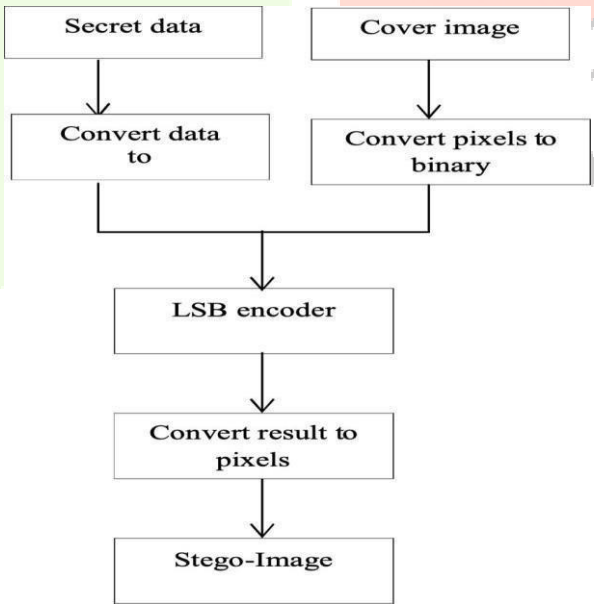
The LSB substitution process involves:

LSB Encoder

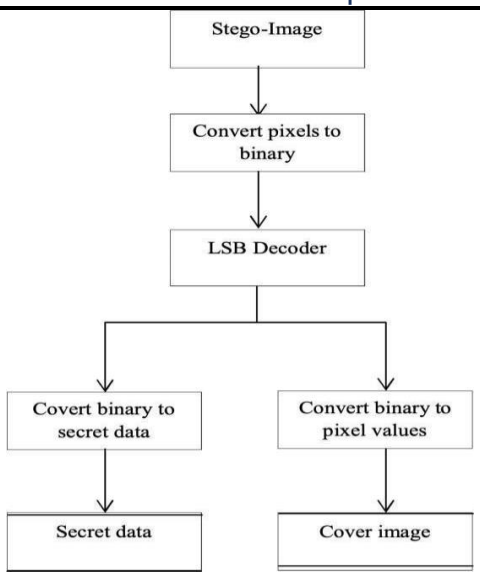
LSB Decoder

The LSB technique serves as the foundation for many methods that hide secret data within carrier data. The encoding process involves hiding the secret data, while the decoding process entails extracting the hidden data.

1. LSB ENCODE :
   a) Input the secret data, whether it's text or an image that needs to be hidden.
   b) Input the cover (original) image of size [256 x 256].
   c) Convert the secret data into binary representation, where each character of text is converted to its ASCII value, or each pixel value of the image is represented in binary.
   d) Convert the pixel values of the cover image into binary representation.
   e) Apply the LSB encoder, whose function is to conceal each bit of the text or image into the least significant bit of each 8 pixel values of the cover image.
   f) Convert the resultant output back to pixel values to obtain the stego-image.

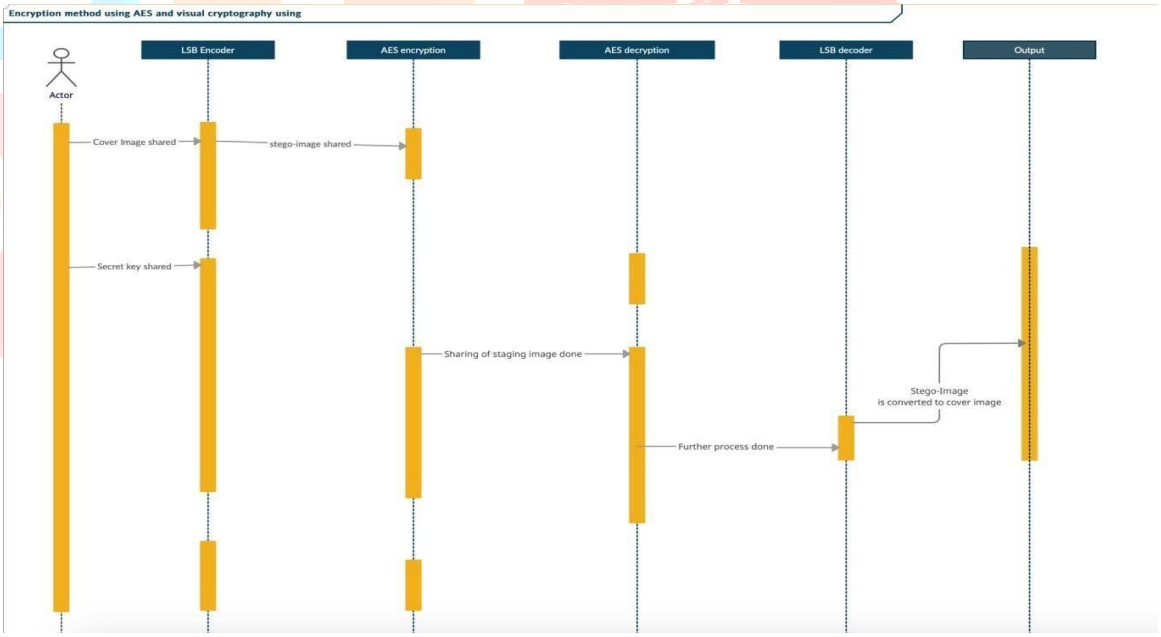



2. LSB DECODER :
   a) Input the stego-image, which contains the hidden data.
   b) Convert the pixel values of the stego-image into binary representation.
   c) Apply the LSB decoder, whose function is to extract the secret data back from the stego-image.
   d) Separate the secret data and the cover image to obtain the desired output.




4.2 SEQUENCE DIAGRAM

The sequence model elaborates on the themes of the use cases. A sequence diagram illustrates an interaction arranged in a time sequence in its logical order. It also depicts the objects participating in the behavior and the messages that they exchange. The sequence diagram of the system under consideration is as shown in the Figure. Initially, the user provides the image, and a secret key is shared with the LSB encoder. Subsequently, it is transferred to the AES encryption method, after which the resulting staged image is forwarded through the communication channel. On the other side, decryption occurs, followed by the transfer of the given steno-image through the LSB decoder, which then converts it into the cover image.




## IV. RESULTS AND DISCUSSION

The proposed data hiding technique provides two levels of security. The first level is achieved by using a simple share creation scheme, and the second level is attained by embedding data inside the shares. Imposters can easily break the system whenever a single level of security is provided. Combining steganography with VC yields effective results with a high level of security. VC requires no computation time for decrypting data and also mitigates the vulnerability of single-level hiding, which is inherent in either

cryptography or steganography. In the proposed method, the combination of VC and steganography not only improves security but also enhances reliability and efficiency.

## REFERENCES


[1] Alexopoulos, C., Bourbakis, N., & Ioannou, N. (1995). Image encryption method using a class of fractals. Journal of Electron- ic Imaging, 43, 251–259.

[2] Bao, G.-J., Ji S.-M., & Shen J.-B. (2002). Magic cube transfor- mation and its application in digital image encryption. Computer Applications, 22(11), 23–25.

[3] Bourbakis, N., & Alexopoulos, C. (1992). Picture data encryp- tion using scan patterns. Pattern Recognition, 25(6), 567–581.

[4] Chang, K.C., & Liu, J.L. (1994). An image encryption scheme based on quad-tree compression scheme. In Proceedings of the 1994 International Computer Symposium, Taiwan, (pp. 230– 237).

[5] Communication theory of secrecy systems. The Bell System Technical Journal, 28, 656– 715.

[6] Ding, W., Yan, W.-Q., & Qi, D.-X. (2000). A novel digital hid- ing technology based on Tangram Encryption. IEEE Proceed- ings of on NEWCAS 2005, and Conways Game. Proceeding of 2000 International Conference on Image Processing (Vol. 1, pp. 601–604), September 2000.