# Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography

Prashanth Kumar Kanchukatla[1], Dr. R.Ramesh Babu[2]
[1]*P.G Student, Digital Electronics and Communication Systems*
[2]*professor, Jagruthi institute of engineering and technology*

***Abstract-*** We present a novel reversible (lossless) data hiding (embedding) technique, which enables the exact recovery of the original host signal upon extraction of the embedded information. A generalization of the well-known LSB (least significant bit) modification is proposed as the data embedding method, which introduces additional operating points on the capacity-distortion curve. Lossless recovery of the original is achieved by compressing portions of the signal that are susceptible to embedding distortion, and transmitting these compressed descriptions as a part of the embedded payload. A prediction-based conditional entropy coder which utilizes static portions of the host as side-information improves the compression efficiency, and thus the lossless data embedding capacity.

## I. INTRODUCTION

Information covering up is an imperative innovation in the zones of data security and sight and sound copyright assurances as it permits the disguise of information inside the computerized media for copyright insurance and information insurance. Numerous plans of information covering up have been proposed to address the issues and difficulties identified with concealing the information, for example, installing limit, intangibility and reversibility.

In this strategy, the information should be consistently covered up or implanted into a transporter or cover flag (sound, pictures, video) in way that makes it difficult for unapproved individuals to get to it [1]. In the advanced imaging area, a few information concealing methods have been proposed [2-4]. In spite of the proficiency of these procedures in ensuring the information, a large portion of them are not equipped for reestablishing the first cover picture upon the extraction of installed information.

This represents a test to applications that require the safeguarding of the cover picture after the concealed information is separated. Appropriately, an extraordinary intrigue has developed in the previous couple of years in the advancement of reversible information concealing (RDH) systems that are equipped for reestablishing the first picture. A few RDH methods have been proposed in the writing and they contend in various viewpoints which incorporate the implanting limit, the nature of the stego picture, size of overhead data and computational unpredictability [2]. For the most part, they can be gathered into three distinct classes dependent on the idea of activity: contrast development, histogram moving, and expectation based strategies. Contrast development (DE) calculations are one well known class of reversible information concealing that are described with low bending and moderately high installing limit.

The primary distinction extension strategy was proposed by Tian in [5]. In this system, the cover picture is divided into a progression of non-covering pixel sets. A mystery bit is then installed utilizing the distinction development of every pixel combine. A few DE-constructed calculations were produced based with respect to Tian's strategy [6-9]. Alattar [6] utilized DE with vectors rather than pixel sets to expand and enhance the execution of Tian's calculation. Hu, et al. proposed a DE-based strategy that enhanced the compressibility of the area delineate. Contrasted with conventional DEbased calculation, their system expanded the implanting limit and performed well with various pictures.

## II. RELATED WORKS

A few calculations used the idea in forecast in information concealing [16-19]. Hong, et al. [16] proposed a reversible information concealing method that depends on picture introduction and the discovery of smooth and complex areas in the host pictures. Li, et al. [17] and Lin, et al. [18] presented a data concealing plan, with reversibility, in view of pixel-esteem requesting (PVO) and forecast blunder development.

One of the principle issues of forecast based reversible information concealing calculations is identified with the sort of the indicator that is utilized to process the expectation blunders. The precision of the indicator influences the inserting limit and the nature of the stego picture. Such huge numbers of indicators were utilized in various information concealing calculations in the writing. Nonetheless, most proposed calculations depend on utilizing a solitary indicator. The goal of this paper is to enhance the productivity of predictionbased reversible information concealing calculations by structuring a calculation that utilizes two indicators to enhance the forecast exactness, along these lines the inserting limit.

The proposed calculation depends on the effective change of forecast mistakes (MPE) calculation; be that as it may, it consolidates two indicators and uses just a single container of the expectation blunders histogram for installing the information, and it is alluded to as 1-Bin MPE2. The1-Bin

MPE2 calculation is additionally stretched out to utilize more expectation mistakes in the inserting stage with the end goal to expand the installing limit. These expansions are alluded to by 2-Bin MPE2 and 3-Bin MPE2 calculations. The execution assessment of the proposed calculation demonstrated its capacity to build the inserting limit with aggressive picture quality. Also, no overhead data is added to adapt to the expansion in the quantity of indicators.

## III. PROPOSED WORK

In this advanced reversible data hiding method, encrypted data can be embedded and extracted from both encrypted images and videos. The data is encrypted using AES algorithm and image is encrypted using the Blowfish algorithm. The proposed work also implements digital video watermarking. Video has become an important tool for the entertainment and educational industry. Digital video watermarking is new technology used for copyright protection of digital media. It inserts authentication information in multimedia data which can be used as proof of ownership. Video watermarking algorithms normally prefers robustness. Most of the proposed video watermarking schemes are based on the techniques of image watermarking. The proposed work includes: generation of encrypted data, generation of encrypted image, data embedding, data extraction and image recovery.

### A. Generation of Encrypted data.

The secret data is encrypted using the AES algorithm. First the secret data is encoded using Huffman Encoding before performing AES encryption. Huffman encoding is performed to compress the secret information and then this information is encrypted using AES algorithm. In this processing step, two main algorithms are used: Huffman Encoding and AES algorithm. Huffman's scheme uses a table of frequency of occurrence for each symbol in the input. This table may be derived from the input itself or from data which is representative of the input. AES is based on a design principle known as a substitution permutation network, combination of both substitution and combination, and is fast in both software and hardware.

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The proposed work utilizes the 128-bit key size of the AES algorithm. Each round consists of four processing steps in which the first step is the substitute byte step and next is the shift row transformation, third is the mix column transformation and last step is the addroundkey transformation step. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

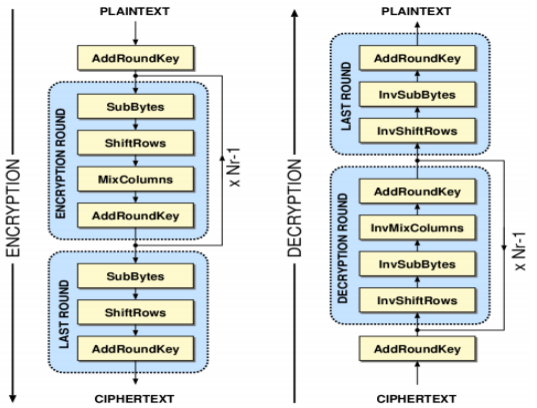


Fig.1: AES Encryption and Decryption

### B. Generation of Encrypted image.

The next step after data encryption is image encryption which is done using Blowfish algorithm. Blowfish is a 64-bit symmetric block cipher that uses a variable-length key from 32 to 448-bits (14 bytes). The algorithm was developed to encrypt 64-bits of plaintext into 64-bits of cipher text efficiently and securely. The operations selected for the algorithm were table lookup, modulus, addition and bitwise exclusive-or to minimize the time required to encrypt and decrypt data on 32-bit processors. Blowfish incorporates a 16 round Feistel network for encryption and decryption. But during each round of Blowfish, the left and right 32-bits of data are modified unlike DES which only modifies the right 32-bits to become the next round's left 32-bits. Blowfish incorporated a bitwise exclusive-or operation to be performed on the left 32-bits before being modified by the F function or propagated to the right 32-bits for the next round. Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation. This operation is different from the permutation function performed in DES.

### C. Reference image hiding in Encrypted image.

After image encryption, the encrypted secret data is embedded into the encrypted image by employing a traditional RDH algorithm like Histogram modification method or a LSB replacement method. Here data embedding is performed in color images. Here each pixel in color images will have three individual components Red(R), Green(G) and Blue(B). The pixel values of these color components will be in the range of [0 255]. The message bits can be embedded in all the three planes and these planes can be recombined to form the original color image. Here the message bits are embedded in every Red component in the RGB plane. After the data embedding is done, the PSNR value is calculated and shown in the textbox in the MATLAB simulator.The proposed work also performs data hiding in videos which can be used for copyright protection of digital media. Here video is divided

into frames and this RGB frames are converted to YUV frames. Frames are sequence of high resolution images and the data embedding is performed by looping of frames.

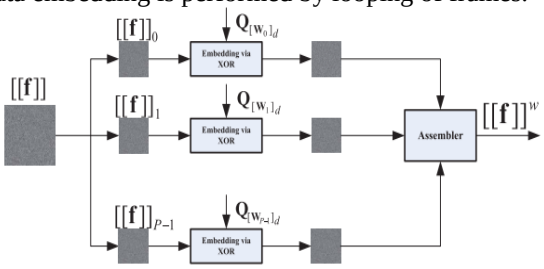


Fig.2: Schematic of data hiding over encrypted domain.

**D. Data Extraction and Image Recovery**

After the data embedding process, the embedded image is obtained along with the PSNR value. The next step is data extraction process which is the reverse of the data embedding process. Here encrypted data is extracted from the encrypted image in the reverse order by employing the AES Decryption algorithm. After that the original image is extracted by using Blowfish Decryption algorithm. After performing the AES Decryption, the Huffman encoded data is retrieved and then Huffman decoding is performed to retrieve the original data. This same process is applied to videos and data extraction and image recovery is successfully separated in videos using the AES algorithm and Blowfish algorithm.

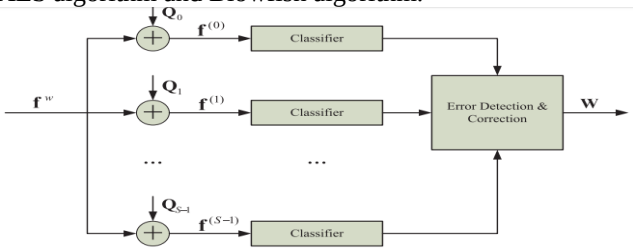


Fig.3: Schematic of the data extraction.

## IV. EXPERIMENTAL RESULTS


Fig.4: Encryption and decryption process with reference image.

In Fig. 4, we see that the capacity of the proposed method depends largely on the characteristics of the host image. Images with large smooth regions, e.g. F-16, accommodate higher capacities than images with irregular textures, e.g. Mandrill. In smooth regions, the predictor is more accurate and therefore conditional residual distributions are steeper. These distributions result in shorter code lengths, and thus higher embedding capacities. The capacity of the scheme increases roughly linearly with number of levels (or exponentially with number of bit-planes). This is due to stronger correlation among more significant levels (bit-planes) of the image. The rate of the increase, however, is not constant either among images or throughout the levels. A direct compression approach that attempts to compress the residual signal alone without utilizing the rest of the image performs significantly worse. For instance, the context-less approach requires an embedding level. A in order to achieve capacities comparable to the presented scheme. The higher embedding level implies significantly higher distortion in the watermark bearing signal.

## V. CONCLUSIONS

An advanced RDH scheme with encrypted data has been presented in this paper. This work combines data encryption with image encryption. The two main algorithms implemented for data encryption and images encryption are the Advanced Encryption Standard (AES) algorithm and the Blowfish algorithm. The work begins with data encoding step which is performed by employing Huffman encoding method and this is done to compress the data. The next step is data encryption which is performed using AES algorithm and after this step the image is encrypted using the Blowfish algorithm which is highly secure because of its longer key length and strongest and fastest nature in data processing compared to other algorithms. Apart from data hiding in images, the proposed work can also performs data hiding in videos which takes this work to a new level in the advanced RDH scheme.

## VI. REFERENCES

[1]. Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, NenghaiYu, and Fenghua Li"Reversible Data Hiding in Encrypted Images byReserving Room Before Encryption" ieee exchanges on data crime scene investigation and security, vol. 8, no. 3, walk 2013.

[2]. M. Goljan, J. Fridrich, and R. Du, "Mutilation free information inserting," in Proc. fourth Int. Workshop on Information Hiding, Lecture Notes in Computer Science, 2001, vol. 2137, pp. 27–41.

[3]. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless summed up LSB information implanting," IEEE Trans. Picture Process., vol. 14, no. 2, pp. 253– 266, Feb. 2005.

[4]. J. Fridrich, M. Goljan, and R. Du, "Lossless information implanting for all picture positions," in Proc. Security and Watermarking of Multimedia Contents IV, Proc. SPIE, 2002, vol. 4675, pp. 572– 583.

[5]. J. Tian, "Reversible information implanting utilizing a distinction development," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890– 896, Aug. 2003 [6] A. M. Alattar, "Reversible watermark utilizing the distinction extension of a summed up whole number change," IEEE Trans. Picture Process., vol. 13, no. 8, pp. 1147– 1156, Aug. 2004.