Secure Reversible Image Data Hiding Over Via Key Modulation

P.Revathi [1], RSVS Aravind[2]

[1]*Pursuing M.Tech (CS) dept. of ECE, Newton's Institute of Engineering College, Alugurajupally, Macherla, Guntur dist., AP, India*

[2]*Associate Professor Dept. of ECE,*
Newton's Institute of Engineering College, Alugurajupally, Macherla, Guntur dist., AP, India

Abstract- **We present a novel reversible (lossless) data hiding (embedding) approach, which allows the exact healing of the unique host sign upon extraction of the embedded information. A generalization of the famous LSB (least good sized bit) change is proposed because the statistics embedding approach, which introduces additional running factors on the potential-distortion curve. Lossless recovery of the original is finished through compressing quantities of the signal which can be vulnerable to embedding distortion, and transmitting these compressed descriptions as part of the embedded payload. A prediction-based conditional entropy coder which makes use of static portions of the host as aspect-information improves the compression performance, and accordingly the lossless facts embedding ability.**

1. INTRODUCTION

Data hiding is an vital technology in the regions of information safety and multimedia copyright protections as it lets in the concealment of facts within the digital media for copyright protection and facts protection. Many schemes of records hiding were proposed to deal with the problems and demanding situations related to hiding the facts, which includes embedding potential, imperceptibility and reversibility.

In this method, the records is meant to be seamlessly hidden or embedded into a service or cowl sign (audio, pix, video) in way that makes it tough for unauthorized human beings to get admission to it [1]. In the digital imaging domain, numerous information hiding techniques had been proposed [2-4]. Despite the efficiency of those strategies in defensive the data, most of them aren't able to restoring the original cowl image upon the extraction of embedded facts. This poses a challenge to applications that require the protection of the cover image after the hidden statistics is extracted. Accordingly, a exquisite hobby has grown within the past few years in the development of reversible records hiding (RDH) strategies which might be able to restoring the original photo. Several RDH strategies were proposed within the literature and that they compete in one of a kind components which include the embedding ability, the great of the stego picture, size of overhead statistics and computational complexity [2]. Generally, they can be grouped into 3 exclusive instructions based on the concept of operation: difference expansion, histogram shifting, and prediction-primarily based strategies. Difference growth (DE) algorithms are one popular elegance of reversible facts hiding that are characterized with low distortion and relatively excessive embedding capability.

The first distinction enlargement technique was proposed through Tian in [5]. In this technique, the duvet photograph is partitioned into a chain of non-overlapping pixel pairs. A mystery bit is then embedded the usage of the difference enlargement of each pixel pair. Several DE-based totally algorithms had been advanced primarily based on Tian's technique [6-9]. Alattar [6] used DE with vectors in place of pixel pairs to increase and improve the overall performance of Tian's algorithm. Hu, et al. Proposed a DE-primarily based approach that improved the compressibility of the place map [8]. Compared to conventional DEbased set of rules, their technique increased the embedding potential and accomplished nicely with special photos.

Another critical class of RDH algorithms are those that are based totally on the idea of histogram moving (HS) [10-13]. Actually, the premise of these algorithms is the work offered by means of Ni, et al.

[13]. In this algorithm, the histogram of the intensities in the unique image is computed. Then, the histogram containers that lie between the height bin and a zero (or minimal) bin is shifted by one in the direction of the zero bin to open space to embedded facts. Afterwards, the name of the game facts bits are embedded by means of enhancing the intensity cost that corresponds to the height only. This technique supplied affordable embedding capacity with minimum peak-signal-to-noise ratio (PSNR) of 48.1 dB. However, the main disadvantage of this method is the confined hiding potential due to the reality that it's far dependent on the pixel rely of the peak value, that is relatively low in herbal photos. Additionally, the embedded secret records can't be recovered without understanding the values of peak and 0 factor of histogram. So the peak and 0 points have to be recorded as overhead or side statistics. Many algorithms have been proposed to beautify the embedding ability of Ni's set of rules even as taking its benefit of manufacturing high first-rate stego pix. Hwang, et al. [10] prolonged Ni's set of rules by the use of two zero factors and one top point of the histogram to embed the records. Lin, et al. [12] hired multilevel hiding approach to acquire high capacity and occasional distortion.

In order to take benefit of the HS strategies in phrases of reversibility, numerous techniques attempted to triumph over the issue of restricted embedding potential by way of extending the approach to histogram of prediction mistakes. Basically, these techniques adjust the values of the prediction errors, which are computed the use of some predictor, rather than the actual intensities. The use of prediction mistakes is motivated with the aid of the fact that these mistakes are sharply targeted close to zero. This implies higher embedding capacities and avoids the want to shop the peaks and zeros when as compared to the authentic HS algorithm. Hong, et al. Proposed extending Ni's algorithm through the usage of the median side detector (MED) [15]. The MED predicator computes the prediction p of pixel x the usage of three neighbouring pixels a, b and c .

Where a, b and c pixels are described with admire to pixel x as proven in Figure 1. Afterwards, the prediction error (PE) that is the difference among pixel price and its prediction is computed. These prediction mistakes are modified based totally on their values and the bits of the secret message. Basically, the mistake values of 0 and -1 are used for embedding best. On different hand, prediction errors greater than 1 and much less than -1 are incremented and decremented by means of 1, respectively. This is finished to loose the histogram bins at 1 and -2 to allow embedding of secret bits with cost of one, while 0 bits are embedded in the zero and -1 packing containers. The changed prediction mistakes are added to the prediction to supply the new values of the pixels inside the stego image, the quilt image after embedding the information. The algorithm confirmed fantastic consequences in phrases of embedding capacity when in comparison to the authentic HS algorithm and it guaranteed a forty eight.1 dB as a lower bound for the first-rate of the stego picture.

2. RELATED WORKS

Several algorithms utilized the idea in prediction in information hiding [16-19]. Hong, et al. [16] proposed a reversible records hiding method that is primarily based on picture interpolation and the detection of smooth and complicated regions in the host photos. Li, et al. [17] and Lin, et al. [18] introduced an information hiding scheme, with reversibility, primarily based on pixel-price-ordering (PVO) and prediction-errors growth.

One of the primary troubles of prediction-primarily based reversible information hiding algorithms is associated with the form of the predictor this is used to compute the prediction errors. The accuracy of the predictor impacts the embedding ability and the excellent of the stego image. So many predictors were utilized in one-of-a-kind information hiding algorithms in the literature. However, most proposed algorithms depend upon the usage of a single predictor. The goal of this paper is to improve the performance of prediction based reversible information hiding algorithms by designing an set of rules that employs predictors to enhance the prediction accuracy, for that reason the embedding capacity.

The proposed set of rules is primarily based at the efficient change of prediction mistakes (MPE) set of rules; but, it carries two predictors and uses most effective one bin of the prediction errors histogram for embedding the facts, and it's far called 1-Bin MPE2. The1-Bin MPE2 set of rules is similarly prolonged to apply greater prediction errors within the embedding section as a way to boom the embedding capacity. These extensions are mentioned through 2-Bin MPE2 and three-Bin MPE2 algorithms. The performance assessment of the proposed algorithm showed its capacity to growth the embedding capability with competitive photograph first-class. Additionally, no overhead statistics is introduced to deal with the growth within the wide variety of predictors.

3. PROPOSED WORK

In this advanced reversible data hiding approach, encrypted statistics can be embedded and extracted from both encrypted pix and movies. The information is encrypted using AES algorithm and image is encrypted the usage of the Blowfish algorithm. The proposed paintings additionally implements virtual video watermarking. Video has become an vital tool for the leisure and educational industry. Digital video watermarking is new generation used for copyright protection of virtual media. It inserts authentication records in multimedia data which can be used as evidence of possession. Video watermarking algorithms commonly prefers robustness. Most of the proposed video watermarking schemes are primarily based at the strategies of photo watermarking. The proposed paintings includes: generation of encrypted information, technology of encrypted photograph, data embedding, statistics extraction and picture recuperation

A. Generation of Encrypted data.

The mystery statistics is encrypted the use of the AES set of rules. First the name of the game facts is encoded the use of Huffman Encoding earlier than appearing AES encryption. Huffman encoding is carried out to compress the name of the game information and then this information is encrypted the use of AES algorithm. In this processing step, two fundamental algorithms are used: Huffman Encoding and AES algorithm. This table can be derived from the enter itself or from records which is representative of the input. AES is based totally on a design precept called a substitution permutation community, aggregate of each substitution and mixture, and is fast in each software program and hardware.

The key size used for an AES cipher specifies the range of repetitions of transformation rounds that convert the enter, referred to as the plaintext, into the very last output, referred to as the ciphertext. The proposed work makes use of the 128-bit key size of the AES algorithm. Each round consists of four processing steps in which step one is the factitious byte step and next is the shift row transformation, third is the mix column transformation and remaining step is the addroundkey transformation step. A set of opposite rounds are carried out to convert ciphertext again into the original plaintext using the equal encryption key.

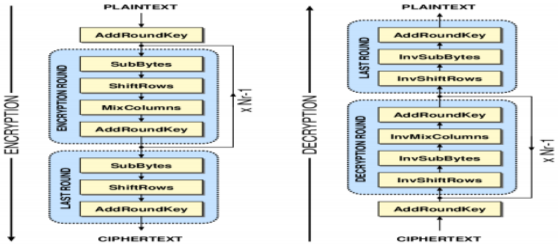

Fig. 1 AES Encryption and Decryption

B. Generation of Encrypted image The next step after records encryption is photograph encryption which is executed using Blowfish algorithm. Blowfish is a sixty four-bit symmetric block cipher that makes use of a variable-duration key from 32 to 448-bits (14 bytes). The algorithm was advanced to encrypt sixty four-bits of plaintext into 64-bits of cipher text efficiently and securely. The operations selected for the set of rules had been desk research, modulus, addition and bitwise specific-or to minimize the time required to encrypt and decrypt information on 32-bit processors. Blowfish incorporates a 16 round Feistel network for encryption and decryption. But in the course of each round of Blowfish, the left and proper 32-bits of statistics are changed in contrast to DES which simplest modifies the right 32-bits to emerge as the following round's left 32-bits. Blowfish integrated a bitwise different-or operation to be achieved at the left 32-bits before being modified through the F feature or propagated to the right 32-bits for the following spherical. Blowfish also included extraordinary-or operations to be accomplished after the 16 rounds and a swap operation. This operation is different from the permutation feature accomplished in DES.

C. Reference image hiding in Encrypted image.

After image encryption, the encrypted mystery data is embedded into the encrypted image by using a conventional RDH set of rules like Histogram amendment approach or a LSB substitute approach. Here records embedding is achieved in shade photos. Here every pixel in colour images could have 3 man or woman components Red(R), Green(G) and Blue(B). The pixel values of these colour additives will be within the range of [0 255]. The message bits can be embedded in all of the 3 planes and these planes may be recombined to form the unique coloration photo. Here the message bits are embedded in every Red factor inside the RGB aircraft. After the records embedding is accomplished, the PSNR price is calculated and proven inside the textbox in the MATLAB simulator.The proposed work also performs data hiding in videos which can be used for copyright protection of virtual media. Here video is divided into frames and this RGB frames are converted to YUV frames. Frames are sequence of excessive resolution snap shots and the information embedding is achieved with the aid of looping of frames.

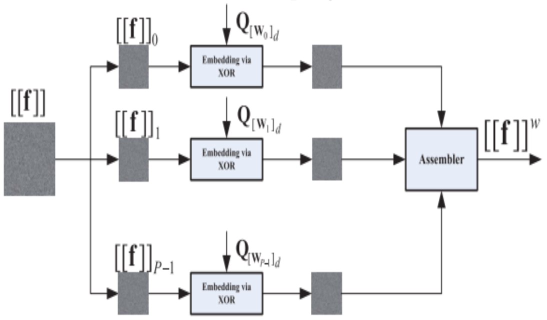

Fig. 2. Schematic of data hiding over encrypted domain.

D. Data Extraction and Image Recovery

After the facts embedding manner, the embedded photograph is acquired at the side of the PSNR fee. The subsequent step is data extraction method which is the reverse of the records embedding manner. Here encrypted data is extracted from the encrypted image in the opposite order by means of using the AES Decryption set of rules. After that the original photograph is extracted by the usage of Blowfish Decryption algorithm. After acting the AES Decryption, the Huffman encoded records is retrieved after which Huffman decoding is finished to retrieve the unique facts. This identical technique is applied to videos and information extraction and picture recovery is successfully separated in films the usage of the AES set of rules and Blowfish set of rules.

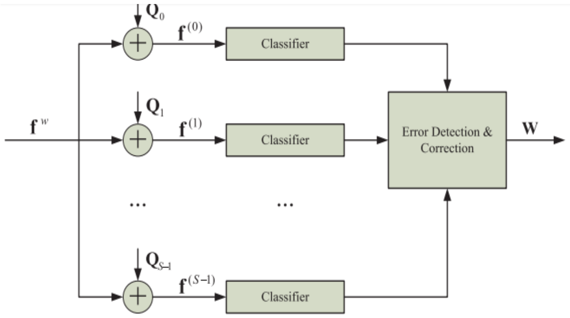

Fig. 3. Schematic of the data extraction.

4. EXPERIMENTAL RESULTS

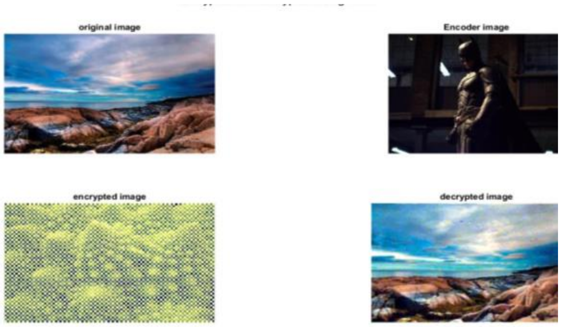

Fig. 4. Encryption and decryption process with reference image.

In Fig. Four, we see that the capacity of the proposed method relies upon largely at the characteristics of the host image. Images with huge easy regions, e.G. F-16, accommodate higher capacities than pix with irregular textures, e.G. Mandrill. In easy regions, the predictor is greater correct and consequently conditional residual distributions are steeper. These distributions result in shorter code lengths, and for that reason better embedding capacities. The capability of the scheme will increase more or less linearly with quantity of stages (or exponentially with quantity of bit-planes). This is due to more potent correlation among more large tiers (bit-planes) of the photo. The rate of the boom, but, isn't consistent both amongst pix or all through the tiers. A direct compression approach that tries to compress the residual signal on my own with out making use of the relaxation of the photograph plays drastically worse. For example, the context-less technique calls for an embedding degree. A with the intention to obtain capacities similar to the supplied scheme. The better embedding degree implies extensively higher distortion in the watermark bearing sign.

5. CONCLUSIONS

An superior RDH scheme with encrypted statistics has been offered on this paper. This work combines information encryption with photograph encryption. The most important algorithms applied for facts encryption and snap shots encryption are the Advanced Encryption Standard (AES) algorithm and the Blowfish set of rules. The paintings starts offevolved with data encoding step that is finished with the aid of using Huffman encoding method and that is accomplished to compress the facts. The subsequent step is information encryption that's accomplished the usage of AES algorithm and after this step the photograph is encrypted the use of the Blowfish algorithm which is pretty relaxed due to its longer key duration and strongest and quickest nature in records processing compared to other algorithms. Apart from records hiding in pictures, the proposed work can also plays information hiding in films which takes this work to a new level in the superior RDH scheme.

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 transactions on information forensics and security, vol. 8, no. 3, march 2013.

[2] M. Goljan, J. Fridrich, and R. Du, “Distortion-free data embedding,” in Proc. 4th 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 generalized- LSB data embedding,” IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005.

[4] J. Fridrich, M. Goljan, and R. Du, “Lossless data embedding for all image formats,” in Proc. Security and Watermarking of Multimedia Contents IV, Proc. SPIE, 2002, vol. 4675, pp. 572–583.

[5] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003

[6] A. M. Alattar, “Reversible watermark using the difference expansion of a generalized integer transform,” IEEE Trans. Image Process., vol. 13, no. 8, pp. 1147–1156, Aug. 2004.

[7] Ratinder Kaur, V. K. Banga "Image Security using Encryption based Algorithm" International Conference on Trends in Electrical, Electronics and PowerEngineering (ICTEEP'2012) July 15-16, 2012 Singapore.

[8] Pia Singh Prof. Karamjeet Singh "Image encryption and decryption using blowfish algorithm in matlab" International Journal of Scientific & Engineering Research, Volume 4,Issue 7, July-2013 150 ISSN 2229-5518.

AUTHORS DETAIL

1. REVATHI P was born in Guntur, AP, and India. She graduated from the Jawaharlal Nehru Technological University Kakinada. Her special fields of interest included communication systems. Presently She is studying M.Tech in Newton’s Institute of Engineering, Macherla.
2. Mr.RSVS Aravind post Graduated in M.TECH in Electronics & Communications in ASTRA (aurora scientific technological and research academy)Hyderabad 2007 to 2009 JNTUH.M.Sc Electronics in ANDHRA UNIVERSITY CAMPUS from 2001 to 2003

   Teaching experience:12years in AEC(AURORA), ASTRA, NOVA , NEWTONS AMIE (Associate member in Institute of Engineers) enrolled on 30-09-2015.

   Presently working as HEAD OF THE DEPARTMENT OF ECE in Newtons Institute of Engineering, macherla.