ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Data Embedding based 4 LSB technique in Image using Steganography

Nitin R. Zinzurke, Prof. Suhas M. Patil

M. E Student, Dept. of Computer Engg., KJCOEMR, Savitribai Phule Pune University, Pune, India

Asst. Professor, Dept. of Computer Engg., KJCOEMR, Savitribai Phule Pune University, Pune, India

ABSTRACT: This technology proposes a lossless, a reversible, and a combined data activity schemes for conversion plain text into cipher text pictures. It is encrypted by public key cryptosystems with probabilistic and polymorphic properties. In the lossless activity, the cipher text pixels square measure replaced with new values of pixels. It is used to implant the extra information into many LSB-planes of cipher text pixels. This process is achieved by multiple layer wet paper for writing. Then, the embedded information may be directly extracted from the encrypted domain. While embedding the data on the secret data is writing on original plaintext image. In the reversible theme, a pre-processing activity should be done is to shrink the image bar graph before image coding. In this process, the modification on encrypted pictures for information embedding won't cause any constituent oversaturation in plaintext domain. In his reversible theme no 100% perfect images, a small distortion are introduced, the embedded information may be extracted and also the original image may be recovered from the directly decrypted image. So as a result of the compatibility between the lossless and reversible technique will performed at the same time performed for the degree of security encrypted image. With the combined technique, a receiver could extract a region of embedded information before secret writing, and extract another part of embedded information and recover the initial plaintext image when secret writing.

KEYWORDS: Data hiding; LSB Algorithm; Image encryption

I. INTRODUCTION

The word steganography comes from the Greek Steganos, which means covered or secret and graphy means writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding secret information in a cover file such that only sender and receiver can detect the existence of the secret information. Secret information is encoded in a manner such that the very existence of the information is concealed.

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not only prevents others from knowing the hidden information, but it also prevents others from thinking that the information even exists. If a steganography method causes someone to suspect there is secret information in a carrier medium, then the method has failed.

The purpose of feasibility study is hiding data secretly for communication with another party. Non detection is more important in audio steganography. As our system is user friendly there can be no difficulty in operating our system. As our system provides technical guarantees of accuracy, reliability, ease of access and data security, it is technically feasible.

From the last few decades of years more working is done on digital area, and the arising topic is steganography for digital media. In normally, the host medium used in steganography includes digital media such as image, text, audio or video etc. A large number of stenographic algorithms have been used for digital media.

II. RELATED WORK

In [1] recently info embedding over footage has drawn tremendous interest, exploitation lossless techniques. Although lossy techniques can allow big concealment capability, host image cannot be recovered with replication. Some

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

applications want precise recovery of the host image, i.e. in medication patient info is embedded whereas not poignant the medical image. Usually lossless info concealment techniques suffer from restricted capability as a result of the host image got to be unbroken intact. Throughout this paper a lossless embedding technique is projected. The projected technique offers concealment capability which can reach up to 5 hundredth of the host image size for footage with big monochromatic regions (cartoons-like). In this, the performance of the novel system is based on algorithms and classifiers. This system is time consuming it cannot detect stage of the cancerous nodule.

In [2] current distinction-expansion (DE) embedding techniques perform one layer embedding in Associate in Nursing passing distinction image. They're doing not intercommunicate sequent distinction image for a further layer embedding unless the current distinction image has no expandable variations left. Supported integer Hare wave retread, we've a bent to propose a replacement initial explicit bedding formula, that utilizes the horizontal additionally as vertical distinction photos for data activity. We've a bent to introduce a projectile expandable distinction search and selection mechanism. This mechanism provides even potentialities to very little variations in two distinctions photos and effectively avoids the case that the most important variations among the first distinction image area unit. System is completely decentralized, fault-resilient, scalable, and reliably. This system detects cancerous nodule but it doesn't calculate its Size as well as stage. Because complexity and infeasible algorithm it's not suitable to implement.

In [3] digital watermarking, generally noted as information activity, has recently been planned as a promising technique for information assurance. Due to information activity, however, some permanent distortion would possibly occur and therefore the initial cowl medium won't be ready to be reversed specifically even once the hidden information square measure extracted out. It's shown that the bulk of the data activity algorithms according at intervals the literature square measure loss. Here, enable US to look at three major classes of data activity formula. With the foremost popularly utilized spread-spectrum water- marking techniques, either in DCT domain or block 8x8 DCT domains, round- off error and or misestimating would possibly happen throughout information embedding. As a result, there is not any because of reverse the stage-media back to the initial whereas not distortion. Attractive features of system include its simplicity, provable correctness, and provable functionality**.** Due to high features included this system required more computation and hardware cost in terms of storage. It does not work on CT images perform only on chest MRI. In [4] author gift a singular lossless (reversible) data-embedding technique, that enables the precise recovery of the initial host signal upon extraction of the embedded knowledge. A generalization of the well-known least very important bit (LSB) modification is projected as a result of the data-embedding methodology that introduces any operative points on the capacity-distortion curve. Lossless recovery of the initial is achieved by pressure components of the signal that unit susceptible to embedding distortion and transmission these compressed descriptions as a region of the embedded payload. This system allows designers to achieve higher performance for a given lung images. This system has more sophistication in maintaining the features of database for each Image. If any updating is done in database then system needs to update the whole database table additionally.

III. SYSTEM OVERVIEW

We say information a knowledge an information activity technique is reversible if the first cowl content will better recovered from the quilt version containing embedded information even supposing a small distortion has been introduced in data embedding procedure. Variety of mechanisms, like distinction enlargement, bar graph shift and lossless compression, are used to develop the reversible information activity techniques for digital pictures. Recently, many smart prediction approaches and optimum transition chance beneath payload-distortion criterion are introduced to boost the performance of reversible information activity.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

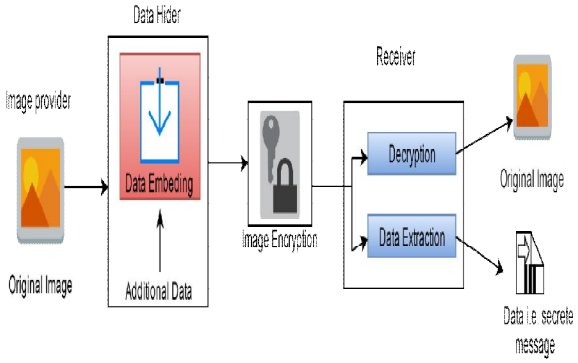

Fig. 1. System Architecture

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded.

Steps of LSB Algorithm:-

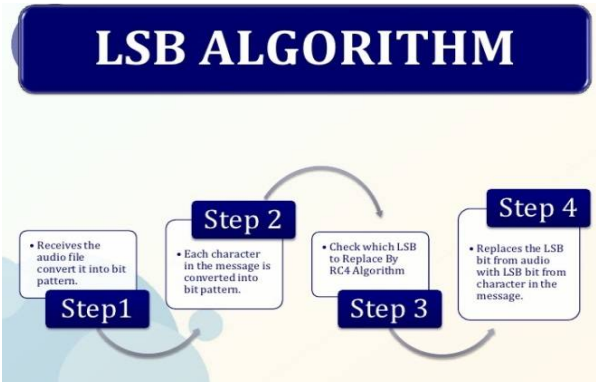

Fig. 2. LSB Algorithm

The following diagram illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method:

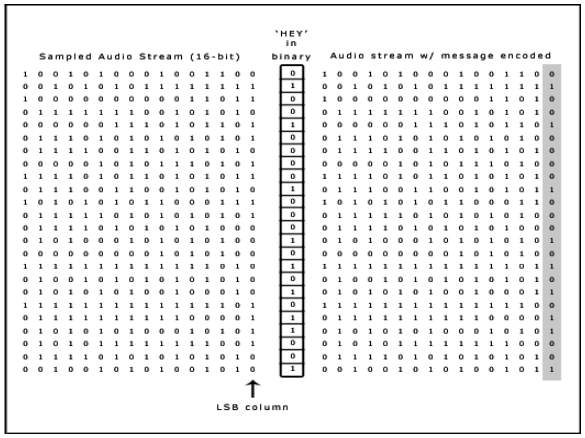

Fig. 3. 'HEY' encoded message

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHZ. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well. Thus, one should consider the signal content before deciding on the LSB operation to use. For example, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise. On the other hand, the same noise would be audible in a sound file containing a piano solo.

To extract a secret message from an LSB encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process. Normally, the length of the secret message to be encoded is smaller than the total number of samples in a sound file. One must decide then on how to choose the subset of samples that will contain the secret message and communicate that decision to the receiver. One trivial technique is to start at the beginning of the sound file and perform LSB coding until the message has been completely embedded, leaving the remaining samples unchanged. This creates a security problem, however in that the first part of the sound file will have different statistical properties than the second part of the sound file that was not modified. One solution to this problem is to pad the secret message with random bits so that the length of the message is equal to the total number of samples. Yet now the embedding process ends up changing far more samples than the transmission of the secret required. This increases the probability that a would-be attacker will suspect secret communication.

IV. MATHEMATICAL MODEL

Let S is the Whole System Consist of

S= {I, P, O}

I = Input

I = {U, IMG}

U = User

U = {u1, u2….un}

IMG = Images

IMG = {img1, img2….imgn}

P = Process:

1. **Image encryption:**
   In this phase, the image provider encrypts a plaintext image using the public key of probabilistic cryptosystem pk.
   For each pixel value m(i, j) where (i, j) indicates the pixel position, the image provider calculates its ciphertext value,
   C(I,j)=E[pk,m(I,j),r(I,j)]
   Where
   E = encryption
   r(i, j) = random value
2. **Data embedding:**
   When having the encrypted image, the data-hider may embed some additional data into it in a lossless manner. For each encrypted pixel, the data-hider selects a random integer r'(i, j) in Z*n and calculates.
   $C'(I,j) = c(I,j).\left(r'(I,j)\right)^{n} \bmod n^2$
3. **Data extraction and image decryption:**
   After receiving an encrypted image containing the additional data, if the receiver knows the data-hiding key, he may calculate the k-th LSB of encrypted pixels, and then extract the embedded data from the K LSB-layers using wet paper coding.
   $C(I,j) = g^{m(i,j)}.\left(r(i,j)\right)^{n} + \underline{\alpha}.n^2.$
   Where, α is an integer.

   Output: Finally the original image will be the output.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

V. RESULTS

Table 1: Results/Analysis

Methodology	4LSB	PSNR	Accuracy
Proposed System	78	86	65
Existing System	60.5	52.5	35

VI. ADVANTAGES AND APPLICATIONS

Advantages:-

1. Utilization of time management.
2. Speedy process
3. Data is highly safe.

Applications:-

1. It can be used in search engine.
2. It can be used in Image sharing sites.

VII. CONCLUSION AND FUTURE WORK

This paper has looked in detail at the major techniques used for data hiding in image files. In section we give an overview of Steganography and in particular the concept of image Steganography. It also described in detail, various Steganography algorithms namely Modified 4LSB Coding, AES for encryption. At the end, feasibility of Steganography was evaluated by considering it's the pros.

In summary, if implemented correctly and in conjunction with cryptographic methods to secure the embedded data before insertion to a cover medium, many of the data hiding methods described above could become powerful tools for the transmission of undetectable and secure communication. This work proposes a lossless, a reversible, and a combined data concealment plans for figure content footage disorganized by open key cryptography with probabilistic and homomorphic properties. Within the lossless arrange, the cipher text element qualities are supplanted with new values for putting in the additional data into the 4LSB-planes of cipher text pixels. Thusly, the put in data may be squarely off from the disorganized space, and also the data implanting operation doesn't influence the unscrambling of distinctive plaintext image. In future, this technique can be processed by using water marking.

REFERENCES

1. N. A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish, 'High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis', Digital Signal Processing, pp. 1629−1636, 2010.
2. J. Tian, 'Reversible Data Embedding Using a Difference Expansion', IEEE Trans. on Circuits and Systems for Video Technology, pp. 890−896, 2003.
3. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, 'Reversible Data Hiding," IEEE Trans. on Circuits and Systems for Video Technology', pp. 354−362, 2006.
4. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, 'Lossless Generalized-LSB Data Embedding', IEEE Trans. on Image Processing, pp. 253–266, 2005.
5. X. Hu, W. Zhang, X. Li, and N. Yu, 'Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding', IEEE Trans. on Information Forensics and Security, pp. 653-664, 2015.
6. X. Zhang, 'Reversible Data Hiding with Optimal Value Transfer', IEEE Trans. on Multimedia, pp. 316−325, 2013.
7. W. Zhang, X. Hu, X. Li, and N. Yu, 'Optimal Transition Probability of Reversible Data Hiding for General Distortion Metrics and Its Applications', IEEE Trans. on Image Processing, pp. 294-304, 2015.
8. S. Lian, Z. Liu, Z. Ren, and H. Wang, 'Commutative Encryption and Watermarking in Video Compression', IEEE Trans. on Circuits and Systems for Video Technology, pp. 774−778, 2007.
9. M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, 'A Commutative Digital Image Watermarking and Encryption Method in the Tree Structured Haar Transform Domain', Signal Processing: Image Communication, pp. 1−12, 2011.
10. X. Zhang, 'Commutative Reversible Data Hiding and Encryption', Security and Communication Networks, 6, pp. 1396−1403, 2013.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

BIOGRAPHY

Nitin Raghunath Zinzurke is a student in the Computer Engineering Department, KJ College of Engineering and Management Research, Savitribai Phule Pune University. He received Bachelor of Engineering (B.E) degree in 2006 from AVCOE Hadapsar, Pune MS, India. His research interests are Image processing, Steganography and information security.

Prof. Suhas M. Patil is an assistant professor in the Computer Engineering Department, KJ College of Engineering and Management Research, Savitribai Phule Pune University.