**Reversible Data Hiding In Encrypted Video Using Context Free Grammar**

By

**Ms. Samiksha k. Velip**

(P. R. No.:-200801130)

Dissertation submitted in partial fulfillment of the requirements for the degree of

**MASTER OF ENGINEERING**

IN

**COMPUTER SCIENCE AND ENGINEERING**

OF GOA UNIVERSITY

*Under the guidance of*

**Dr. J. A. Laxminarayana**



**June 2017**

**COMPUTER ENGINEERING DEPARTMENT**

**GOA COLLEGE OF ENGINEERING**

(GOVERNMENT OF GOA)

**FARMAGUDI, PONDA, GOA - 403401**

**Dissertation Approval Sheet**

The dissertation entitled **“Reversible Data Hiding In Encrypted Video Using Context Free Grammar”** by Ms. Samiksha Velip completed in the year 2016-17 is approved as a partial fulfillment of the requirements for the Degree of **MASTER OF ENGINEERING in COMPUTER SCIENCE AND ENGINEERING**, and is a record of bonafide work carried out successfully under our guidance.

Ms. Samiksha k. Velip has one number of Conference/ publications in the relevant area of the “Dissertation”.

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (Internal Examiner )  Dr. J. A. Laxminarayana  Computer Engineering Department  Goa College of Engineering |  |

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (Head of Department)  Dr. J. A. Laxminarayana  Computer Engineering Department  Goa College of Engineering | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (Principal)  Goa College of Engineering |

Date: /0 /2017

**CERTIFICATE**

This is to certify that the dissertation

# Reversible Data Hiding In Encrypted Video Using Context Free Grammar

Submitted by

# Ms. Samiksha K. Velip

(P. R. No.:- 200801130)

Has been successfully completed and defended in the academic year 2016-2017 as a partial fulfillment of the requirement for the Degree of MASTER OF ENGINEERING in Computer Science and Engineering, at Goa College of Engineering, Farmagudi, Goa.

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Internal Examiner** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **External Examiner** |

**Place: Goa College Of Engineering, Farmagudi**

**Date: /0 /2017**

**CONTENTS**

|  |  |  |
| --- | --- | --- |
|  | **Title** | **Page No.** |
|  | **Acknowledgement** | **(i)** |
|  | **Abstract** | **(ii)** |
|  | **List Of Figures** | **(iii)** |
|  | **List Of Abbreviations** | **(iv)** |
|  |  |  |
| **Chapter 1** | **Introduction** | **1 – 6** |
| 1.1 | Preamble | 1 |
| 1.2 | Objectives | 3 |
| 1.3 | Scope | 3 |
| 1.4 | Motivation | 4 |
| 1.5 | Hardware and Software Requirements | 5 |
| 1.5.1 | Hardware Requirements | 5 |
| 1.5.2 | Software Requirements | 5 |
| 1.6 | Organization of the Report | 5 |
| 1.7 | Summary | 6 |
|  |  |  |
| **Chapter 2** | **Literature Survey** | **7 – 13** |
| 2.1 | Reversible Data Hiding In Encrypted Video | 7 |
| 2.2 | Reversible Data Hiding In Encrypted Image | 8 |
| 2.3 | Reversible Data Hiding In Audio | 11 |
| 2.4 | Context Free Grammar | 12 |
| 2.8 | Outcome of Literature Survey | 13 |
| 2.9 | Summary | 13 |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Chapter 3** | **Proposed Work** | **14-15** |
| 3.1 | Problem Definition | 14 |
| 3.2 | Project Specification | 14 |
| 3.3 | Summary | 15 |
|  |  |  |
| **Chapter 4** | **System Design** | **16-23** |
| 4.1 | Overview of the Proposed Design to Achieve the Desired Objectives | 16 |
| 4.2 | Proposed Design Methodologies | 18 |
| 4.2.1 | Encrypted Image Generation | 18 |
| 4.2.2 | Data Hiding In Encrypted Image | 20 |
| 4.2.3 | Data Extraction And Image Recovery | 23 |
| 4.3 | Summary | 23 |
|  |  |  |
| **Chapter 5** | **Implementation and Results** | **24-30** |
| 5.1 | Encrypted Image Generation | 24 |
| 5.2 | Data Hiding In Encrypted Image | 27 |
| 5.3 | Data Extraction And Image Recovery | 28 |
| 5.4 | Summary | 30 |
|  |  |  |
| **Chapter 6** | **Conclusion And Future Work** | **31** |
| 6.1 | Conclusion | 31 |
| 6.2 | Future Work | 31 |
|  |  |  |
|  | **Bibliography** | **32** |
|  | **Publications** | **35** |

**ACKNOWLEDGEMENT**

I acknowledge the support of **Prof. (Dr.) V.N. Shet** the Principal of Goa College of Engineering, Farmagudi for providing all the facilities to meet my project requirements and for being a constant source of encouragement.

I also take this opportunity to convey my sincere thanks to **Prof. (Dr.) J.A. Laxminarayana,** the Head of the Computer Engineering Department, Goa College of Engineering for his constant guidance, support and valuable suggestions.

The completion of our project could not have been accomplished without the valuable guidance from my guide **Prof. (Dr.) J.A. Laxminarayana,** Computer Engineering Department, Goa College of Engineering. I am immensely grateful to him for his encouragement, motivation and valuable suggestions throughout the interesting and enriching path of our thesis. I deeply appreciate every effort he put to bring my project to success.

My special thanks to my parents and classmates for being the perennial source of encouragement and support which motivated me to work to my full potential.

Finally, I thank all my teachers for their valuable guidance which always kept me growing and all the non teaching staff of Computer Engineering Department, Goa College of Engineering, for their kind cooperation during the period of my project.

**ABSTRACT**

The main motivation behind reversible data hiding is to improve the security of cover image as well as the secret message to be hidden in a given cover image. The security plays an important role in the transmission of confidential data over the internet. So, as a part of improving security in data transmission, we will hide the data inside an encrypted video. Thereby, confidentiality of the image, as well as the embedded data is maintained.

The proposed method ensures the security of secret message by using a context free grammar. Given secret message is converted into a sequence of context free grammar production rules and these rules are embedded into encrypted key frame images. On the other side when user decrypts this key frame images, the user uses Purdom’s algorithm to parse this production rules and to get the original message back.

The proposed method provides total data security and reversibility.

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **Figure No.** | **Title** | **Page No.** |
| 4.1 | Overview of the Proposed Method | 16 |
| 4.2 | LSB substitution | 19 |
| 5.1 | Video partition-Image frames | 24 |
| 5.2 | Key-frame selection | 25 |
| 5.3 | Reserve Room Before Encryption (RRBE) | 25 |
| 5.4 | Image Frame before encryption | 26 |
| 5.5 | Image encryption using RSA algorithm | 26 |
| 5.6 | Generate CFG for input text | 27 |
| 5.7 | Data embedded in encrypted image | 28 |
| 5.8 | Data embedded in encrypted image | 28 |
| 5.9 | CFG extraction from encrypted image | 29 |
| 5.10  5.11 | Parsing of CFG  Image decryption | 30  30 |

**LIST OF ABBREVIATIONS**

|  |  |
| --- | --- |
| RDH | Reversible Data Hiding |
| LSB | Least Significant Bit |
| AES | Advanced Encryption Standard |
| RSA | Rivest, Shamir and Adleman Adleman |
| CFG | Context Free Grammar |
| PSNR | Peak Signal Noise Ratio |
| MSE | Mean Squared Error |
| IPM | Intra-Prediction Mode |
| MVD | Motion Vector Difference |
|  |  |
|  |  |

**Chapter 1**

**Introduction**

* 1. **Preamble**

Data hiding is a group of techniques used to hide a secret information in a host media (like audio, images, video) with a small deterioration in host media and then later use secure means to extract hidden secure information. For example, steganography, watermarking, and cryptography. Data hiding techniques are classified as follows.

1. **Steganography and Cryptography**

The word steganography is derived from the Greek word meaning “covered writing”. Steganography is defined as hiding a secret message within another media so that the presence of the hidden message is obscure. The key idea behind steganography is that the message to be transmitted is not detectable to the casual eye.

Cryptography is a technique used to communicate and to store information or data privately and securely, without being intercepted by third parties. This includes processes such as hashing, encryption, digital signature, and steganography.

The difference between steganography and cryptography is that in cryptography, one can state that a message has been encrypted, but he/she cannot extract the message without knowing the encryption key.

 In steganography, the message may not be difficult to extract, but it is difficult to detect the presence of the message hidden in an image. When combined, steganography and cryptography can provide two levels of security.

1. **Reversible Data Hiding (RDH)**

In this technique the secret message and the original cover image can be recovered without any distortion present in it.

Such system contains a cover image, encryption key, secret information, and data hiding key. The cover image is encrypted, secret information is embedded and then image is sent to intended receiver. Receiver on the other side will decrypt the encrypted image and extract the secret message. The term reversible in RDH is defined as, the extraction of secret information embedded in the encrypted cover image as well as image decryption without any data loss.

1. **Separable Reversible Data Hiding**

The term separable in RDH is defined as “capable of being separated or dissociated”. In other words, separate some activities or process using specific rules. In separable RDH concept, two processes that can occur independent of each other at receiver side are

1. Extraction of data embedded in image.
2. Decryption of encrypted image

A data hiding system is characterized using four different aspects: capacity, security, perceptibility and robustness.

1. **Capacity**: The amount of information that can be hidden in the cover image.
2. **Security**: The inability of the hacker to extract hidden information.
3. **Perceptibility**: The inability to detect the hidden information.
4. **Robustness**: The amount of modification the stego-image can withstand before the hidden information is destroyed.
   1. **Objectives**

The main goal of reversible data hiding is to secure communication. So, a fundamental requirement of this RDH system is that the secret message carried by cover-image should not be detectable to human beings.

Main objective of this project is

1. Reserve space in cover image to embed data.
2. Enhance image security.
3. Generate Context Free Grammar (CFG) based on input text.
4. CFG parsing using Purdom’s algorithm.
   1. **Scope**

Now-a-days security is the major concern for data communication over an insecure network. A digital image and information embedding system have a number of important multimedia applications. These systems embed information or signal (embedded signal) within another medium or signal (Host Signal).

Recently more attention is paid to reversible data hiding (RDH) since it maintains the excellent property that the original cover image can be recovered losslessly after extracting hidden data while preserving the confidentiality of cover image. The embedded data can be extracted from the cover image without any glitch.

The major application of this method is medical imagery and military where confidentiality of data and cover image should be maintained. The most secure way to achieve this confidentiality is to use separate keys in case of encryption and data hiding on sender and receiver side.

Sensitive information like net banking transaction or documents like bank checks are scanned, protected with an authentication scheme based on a reversible data hiding, and sent through the Internet. In most cases, the watermarked documents are ample to distinguish unequivocally the contents of the documents. However, if any uncertainty arises, the possibility of recovering the original, unmarked document is very interesting. Using reversible data hiding (RDH) technique, the original cover image can be losslessly recovered after extracting hidden information while maintaining the confidentiality of image content**.**

Few applications of reversible data hiding is

* Covert communication using images.
* Ownership of digital images, authentication, copyright.
* Data integrity, fraud detection, self-correcting images.
* Traitor-tracing (fingerprinting video-tapes).
* Adding captions to images, additional information such as subtitles, to video, embedding subtitles or audio tracks to video (video-in-video).
* Intelligent browsers, automatic copyright information, viewing a movie in a given rated version.
* Copy control (secondary protection for DVD).
  1. **Motivation**

The main motivation behind the development of software is to enhance the security of the hidden data in the encrypted image. There hasn’t been much work done in reversible data hiding to provide security to embedded data in the encrypted image other than using data hiding key. This is just an endeavor to make the hidden data more secure and can be extracted without any distortion.

Although much work is carried out in reversible data hiding, their main focus was to secure the cover image or RDH technique used. The main question is “what if the hacker obtains the data hiding key??” because once the hacker is vigilant of data hiding key, he/she can facilely intercept the hiding message hence a breach of security. Therefore this system is using context free grammar instead of plain text as CFG is very difficult to intercept.

This software also uses RSA algorithm to encrypt image frames. The main advantage of using RSA algorithm is that it uses separate keys for encryption and decryption. Even if the hacker obtains the encryption key, it’s very difficult to predict the decryption key.

* 1. **Hardware and Software Requirements**
     1. **Hardware Requirements**
* Intel Core i3 processor
* Minimum 4 GB RAM
* Minimum 500GB Hard Disk space for data
  + 1. **Software Requirements**
* Windows 7 Professional
* MatlabR2015a
  1. **Organization of the Report**

The report is organized in 6 chapters in total.

Chapter 2 covers the Literature Survey, which explains various techniques that have been adapted in the past for reversible data hiding in encrypted image. Chapter 3 states the proposed work with the problem definition and specification. Chapter 4 explains the detailed design methodology to achieve the objectives. In this chapter the modules of the project are explained. Chapter 5 explains the implementation details and the experimental results of the project. Finally, Chapter 6 states the conclusion analyzing the project.

* 1. **Summary**

The main focus of the chapter was on explaining the objective, scope and motivation behind carrying out this thesis work. The hardware and software requirements required for the project were also stated. Also the basic organization of the report was described.

**Chapter 2**

**Literature Survey**

* 1. **Reversible Data Hiding in Encrypted Video**

Gayatri Pisal et al. devised an RDH method in the encrypted video. In this system, authors utilize the technique of Reserving Room Before Encryption (RRBE) to surmount the drawbacks of existing system i.e. the cover image was decrypted with some distortions in it. The content owner first encrypt the cover image and pass it to data hider who will embed secret message in cover image using data hiding key. On the other side receiver will use data hiding key to extract hidden message and encryption key to extract cover image back without any distortion. [1]

In [2], a novel scheme of data hiding directly in the encrypted version of H.264/AVC video stream is proposed, which includes the following three components, i.e., H.264/AVC video encryption, data embedding, and data extraction.

To start with, the client scrambles the first H.264/AVC video stream utilizing standard stream figures with encryption keys to create an encoded video stream. This is accomplished by scrambling the codewords of IPMs, the codewords of MVDs, and the codewords of lingering coefficients. Encryption of codewords of IPMs is achieved by selecting IPMs in the Intra\_4×4 and Intra\_16 × 16 blocks for encryption. The motion vectors should be encrypted in order to protect both the texture and motion information. To enhance the security of the system, the residual data in both Iframes and P-frames is encrypted. Without knowing the video content, the client implants the extra data into the encoded video stream by using codeword substituting technique.

The codewords substitution should fulfill the following limitation.

1. The bitstream after codeword substituting should be syntax docile so that it can be decoded using the standard decoder.
2. Bit-rate should be same i.e. the substituted codeword should be of same size as the original codeword.

At the receiver side, data extraction can be achieved either in encrypted or in decrypted mode.

* 1. **Reversible Data Hiding In Encrypted Image**

T. Margaret devised an RDH method in an encrypted image utilizing XOR cipher technique to locate the maximum PSNR value and hiding capacity with less MSE. This process requires a cover image to hide secret information, secret information which is scrambled utilizing the encryption key..

The cover image is encoded using XOR ciphering. After completion of data embedding process, the PSNR value and MSE are obtained.

PSNR is usually expressed in terms of the logarithmic decibel scale.

PSNR is most effectively characterized through the mean squared mistake (MSE).

The results obtained specify that RGB image has higher PSNR and MSE value compared to grayscale and binary image [3].

In [4], a novel scheme of secured data transmission by scalable compression is used. In this paper, the author embeds the cover image with copyright information using RDH technique by RRBE method. For secure image transmission, steganography and scalable compression algorithm are applied.

This method has 3 phases on sender side:

1. reversible data hiding by RRBE
2. scalable compression
3. Data hiding

Receiver side process involves:

1. inverse RDH
2. inverse scalable compression
3. data-image extraction

In [5], authorsare using technique called “Rhombus method” to vacant space before encryption in the cover image. Later this image is encoded and reserved space is utilized to hide secret information in the cover image.

In rhombus method to predict the pixels value Aij, the neighboring 4 pixels of Aij are used that composes a rhombus. These five pixels comprise a cell which is utilized to hide one bit of information. For data embedding, even and odd bits are utilized. Error e is calculated based on the value of Aij.

In image encryption phase, XOR method is used where the encryption key is XOR with each bit of an image.

In [6], author devised a non-separable data hiding method using chaoutic map. First, a user takes the inverse s-order of the cover image. Later this image is given to data hider who encodes the additional data into the cover image using data hiding key and then this image is encrypted with the avail of encryption key.

As the term non-separable specifies that activities cannot be separated, the receiver first has to decrypt the cover image in order to extract data and then data extraction take place.

The PSNR values acquired from decoded image are same as the cover image before decryption. In this manner, data extraction and image recovery are lossless.

In [7], authors propose a novel scheme of reversible data hiding (RDH) in encrypted images using distributed source coding (DSC). The content owner encodes the cover image using the stream cipher. Later data hider compresses a series of selected bits from the encrypted cover image to make room for the secret information. The selected bits are encoded using low-density parity check (LDPC) codes. This is done by selecting and compressing some MSB of the secret image using LDPC codes to create an extra space and embeds additional bits into the encrypted image using the data hiding key.

On the receiver side, if a recipient has both the encryption and data embedding keys, the beneficiary can separate the compressed bits, and implement the distributed source decoding using the estimated image as side information to perfectly recuperate the original image back.

In [8], the authors present a reversible data hiding scheme based on histogram modification. To begin with, the input image is isolated into a number of blocks and then histogram shifting is done on each block which improves the information concealing limit and visual quality. The Second stage known as processing stage includes generation of the histogram for each block and calculating the difference after histogram modification.

After processing stage comes the embedding stage where first binary tree level is found. Then for each block

a) Narrow the histogram in the range 2L, 255-2 L by shifting the histogram from both sides.

b) Scan the image block in the inverse-S order and find the difference between adjacent pixel values.

c) Then scan the image block in the same order and if difference value di is greater than 2L, shift by 2 L units.

The result shows that distortion of an image increases with rise in the value of binary tree level L.

In [9], the authors propose a method of RDH in encrypted images (RDH-EI) based on progressive recovery. The sender encodes the cover image using a stream cipher algorithm and transfers ciphertext to the server. The data-hider on the server separates the encrypted image into three channels and respectively embeds different amount of additional bits into each one to create a stamped encoded picture.. The pixels of the ciphertext image are divided into three sets: the Square, the Triangle, and the Circle. Hence, there are MN/4 pixels in the Square set, MN/4 pixels in the Triangle set, and MN/2 pixels in the Circle set. With an embedding key KEMB, the data-hider pseudo-randomly permutes the encrypted pixels within each set. On the recipient side, an additional message can be removed from the marked encoded image, and the original image can be recouped with no blunders.

* 1. **Reversible Data In Audio**

Akira Nishimura proposed an RDH technique in audio using linear prediction and error expansion. The proposed method is superior in terms of having a smaller loss of payload data and little objective quality degradation on average. In this paper, three means are proposed to improve the conventional prediction error expansion techniques for reversible data hiding of audio waveforms. Firstly, errors when deriving the predicted amplitudes are reduced by using real number calculations and then rounding the resulting output, so that the quality degradation of the stego audio is minimized. Secondly, no location map is used to prevent amplitude overflow, resulting in the method achieving a storage capacity of nearly 1 bit per sample of payload data. Finally, concealment of payload data is realized by autoregressive coefficients and/or an exclusive or (XOR) operation on the secret key for the LSB of the initial stego samples. [10]

In [11], the authors devised a novel scheme for reversible data hiding scheme for digital audio by using non-causal prediction of alterable orders. Firstly, the samples in a host signal are divided into the cross and the dot sets. Then, each sample in a set is estimated by using the past P samples and the future Q samples as prediction context. The order P+Q and the prediction coefficients are computed by referring to the minimum error power method. With the proposed predictor, the prediction errors can be efficiently reduced for different types of audio files.

* 1. **Context Free Grammar**

In [12], authors devised a simple approach to test grammar by deriving the quantity of sentences from the linguistic use under test and to approve whether they agree to the intended language. In this paper, an improved algorithm which incorporates a length control mechanism into the generation process to produce more and simpler sentences is proposed. According to an existing algorithm (Purdom algorithm) which produces too few sentences are long and complex. These sentences are not exceptionally perfect for building a test set for the linguistic use.

For this reason, authors propose an improved algorithm which generates more and simpler sentences that might be beneficial for testing. If the length of a sentence is restricted in a certain size, then the number of rules covered by it is also limited. This confinement won't just abstain from creating too long sentences but also make the coverage of rules spread out among more sentences other than concentrated in a small amount.

In [13], the authors are interested in context-free grammars G in which L(G) consists of exactly one string. Given **a** data string z over **a** finite alphabet and a context-free grammar G such that *L(G)* = {z}, one can reduce G to a simpler grammar G’ for which *L(G’)* = {z} and for which certain constraints are satisfied.

One then losslessly compresses z by losslessly compressing the grammar G’. The redundancy performance of this compression algorithm based upon reduced grammars is discussed.

To simplify the grammar the following two constraints on the grammar G are imposed:

1. In the right-hand sides of the production rules of the grammar, there can be no substring of length two that shows up in two non-covering positions.
2. Every non-terminal symbol of the grammar (except S) must show up at any rate twice on the right-hand sides of the generation standards of the linguistic use.
   1. **Outcome of Literature Survey**

Context-free grammar and reversible data hiding were studied for audio, video, and image. The most commonly used method in reversible data hiding is Reserve Room Before Encryption (RRBE) as cover images can be extracted without any distortion in it.

Other reversible data hiding methods used for data embedding are difference expansion (DE), histogram shifting (HS), LSB method etc.

* 1. **Summary**

This chapter outlines the previous work done in reversible data hiding in an encrypted video, audio, and image as well as work is done on context-free grammar to generate sentences and to also parse it.

**Chapter 3**

**Proposed Work**

* 1. **Problem Definition**

As a new trend, reversible data hiding in encoded images allows the service provider to hide additional information, e.g., image metadata, labels, notations or authentication information, into the encoded images without accessing the original contents. The original image is required to be perfectly recovered and the hidden message completely extracted on the receiving side.

* 1. **Problem Specification**

In RDH system, an input video is partitioned into multiple image frames for hiding secret information. This secret information is used as a covert communication between two parties. The secret information is converted into a set of context-free grammar production rules which provide security to hidden data.

On receiver side, after data extraction, these production rules are parsed to get the original input back. Purdom algorithm is used for CFG parsing. Extracted data is error free.

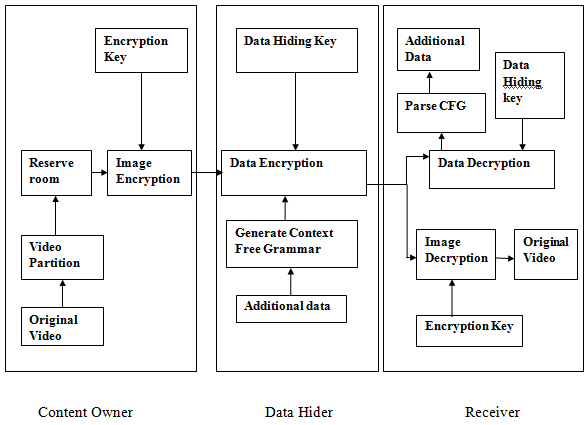
* 1. **Summary**

The actual problem that will be solved in this thesis work was defined. A brief specification of the problem and the method which will be used to solve this problem was described.

**Chapter 4**

**System Design**

* 1. **Overview of the Proposed Design to Achieve the Desired Objectives**

****

**Figure 4.1:** Overview of the Proposed Method

In Figure 4.1 the overall model of the proposed method is described. Initially an input video is received from the user and divided into many image frames. Then some space is reserved in key-frame images to embed secret data using LSB method. Later the image frames are encrypted using RSA algorithm. The encrypted image frames are passed to the data hider so that some data can be embedded in the key frames. Data hider first generates context-free grammar rules based on input message and then these rules are embedded in key-frame images.

On the other side, the receiver will use data hiding key to extract the hidden data and then Pudom’s algorithm is used to parse the context-free grammar rules to get the original message back.

The receiver uses private key to decrypt the image frames and merge it to get the original video back.

If the receiver has only data hiding key, then he/she can only extract hidden data and parse to get original message back. If the receiver has private key then he/she can only decrypt the image frames to get the original video back. Only if the receiver has both data hiding key and private key, he/she can intercept the hidden message and exactly recover the original images back.

* 1. **Proposed Design Methodologies**

In this project video and text message is taken as an input, where text is converted to CFG and embedded in image frames.

* + 1. **ENCRYPTED IMAGE GENERATION**

1. **Video Partition**

At the beginning, the original video is divided into a number of image frames. Key-frames are selected in which we will hide secret data.

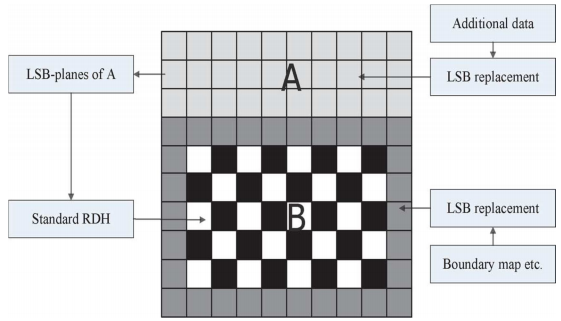
**Algorithm key frame selection**

%calculating mean and standard deviation and extracting frames

1. Mean = mean2(X)
2. Std = std2(X)
3. Threshold = std+mean\*4
4. For g=1: T
5. Read first image key frame
6. if (g~=xyloObj.NumberOfFrames)
7. Read Next key frames
8. Th = difference(p,J);
9. If ( th > Th) % Greater than threshold select as a key frame
10. display image
11. **Image Partition**

Image partition step divides original image into two parts **A** and **B**.

The LSBs of **A’s** are reversibly embedded into **B** with a standard RDH algorithm so that LSBs of **A** can be used for accommodating messages; at last, encrypt the rearranged image to generate its final version. For example assume the original image C is a gray-scale image with its size M x N, it is divided in to two equal sized images. In this the B part has the smoother area to apply the RDH technique. The LSBs of the pixels of A where the data is hiding is stored.



**Fig 4.2: LSB substitution**

1. **Image Encryption**

After performing image partitioning step to vacate some space, images frames are encrypted using an encryption key. After content owner encrypts the image frames, these frames are given to data hider/ database manager or the content owner himself can embed additional data in encrypted images.

**Algorithm Image Encryption (RSA Algorithm)**

**Key Pair Generation**

1. Generate two large random primes, *p* and *q*, such that n = p\*q is of the required bit length, e.g. 1024 bits.
2. Compute n = p\*q and Ф(n) = (p-1)\*(q-1).
3. Choose an integer *e*, 1 < e < phi, such that gcd(e, Ф(n)) = 1.
4. Compute the secret exponent *d*, 1 < d < phi, such that ed ≡ 1 (mod Ф(n)).
5. The public key is (n, e) and the private key (d, p, q).

* n is known as the *modulus*.
* e is known as the *public exponent* or *encryption exponent* or just the *exponent*.
* d is known as the *secret exponent* or *decryption exponent*.

**Encryption**

1. Computes the ciphertext c = me mod n

**Decryption**

1. Compute m = cd mod n.
   * 1. **DATA HIDING IN ENCRYPTED IMAGE**

After producing the encrypted image, the owner hands over it to a data hider (e.g., a database manager) so that the data hider can embed some auxiliary data.

1. **Generation of Context Free Grammar**

Secret data to be embedded is in plain text form which is very insecure. In order to prevent it from getting hacked the input message is hidden in form of context-free grammar, which when parsed by intended user can intercept the message.

1. **Data Hiding**

Using the data hiding key additional data/secret data is embedded into encrypted image frames. After data hiding, all image frames are combined (video) and send to intended user.

**Algorithm Data Hiding (LSB method)**

Inputs : Cover image, stego-key and the text file

Output: stego image

Procedure Step 1: Extract the pixels of the cover image.

Step 2: Extract the characters of the text file.

Step 3: Extract the characters from the data hiding key.

Step 4: Choose first pixel and pick characters of the Stego key and place it in first component of pixel.

Step 5: Place some terminating symbol to indicate end of the key. 0 has been used as a terminating symbol in this algorithm.

Step 6: Insert characters of text file in each first component of next pixels by replacing it.

Step 7: Repeat step 6.

Step 8: place terminating symbol to indicate end of data.

Step 9: Obtained stego-image.

For example, suppose one can hide a message in three pixels of an image (24-bit colors).

Suppose the original 3 pixels are:

11101010 11101000 11001011

01100110 11001010 11101000

11001001 00100101 11101001

To hide the letter ”J” which has a position 74 into ASCII character set and have a binary representation ”01001010”, by altering the channel bits of pixels.

11101010 11101001 11001010

01100110 11001011 11101000

11001001 00100100 11101001

For this situation, just four bits should have been changed to embed the character successfully.

The subsequent changes that are made to the minimum noteworthy bits are too little to be perceived by the human eye, so the message is viably covered up. The preferred standpoint of LSB installing is its effortlessness and numerous strategies utilize these techniques

Now the final video contains hidden message used as secret communication.

* + 1. **DATA EXTRACTION AND VIDEO RECOVERY**

1. **Data Extraction**

Using data hiding key, the receiver first extracts the hidden message (production rules), merge it and then parse it using Purdom’s algorithm to get original message back.

**Algorithm Purdom’s algorithm (CFG Parsing)**

1. Stack.push(S0) //S0 is the start symbol
2. While not stack.empty() do
3. s ← stack.pop()
4. If s is terminal then
5. Print s
6. Else
7. (p = s **→ α )** ← choose a rule for s
8. Stack.push(reverse(α))
9. End if
10. End while
11. **Video Recovery**

Using encryption key, the user will decrypt the image frames and merge it to get the original video back.

* 1. **Summary**

The detailed design flow was described. The various algorithms that are to be followed at each step in the design were discussed.

**Chapter 5**

**Implementation and Results**

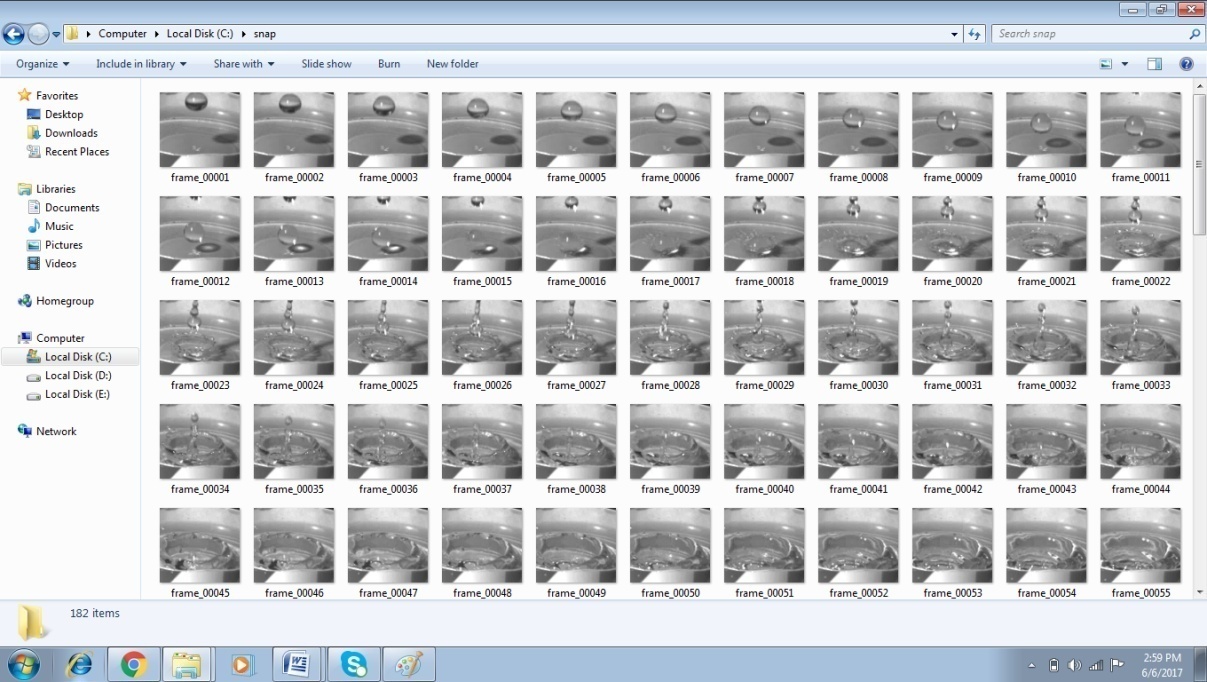
In this chapter the detailed implementation of the reversible data hiding in encrypted video using context free grammar using Matlab r2015a is discussed.

* + 1. **ENCRYPTED IMAGE GENERATION**

Step 1: Video Partition

Input: drop.avi video

Output: video is divided into 182 frames

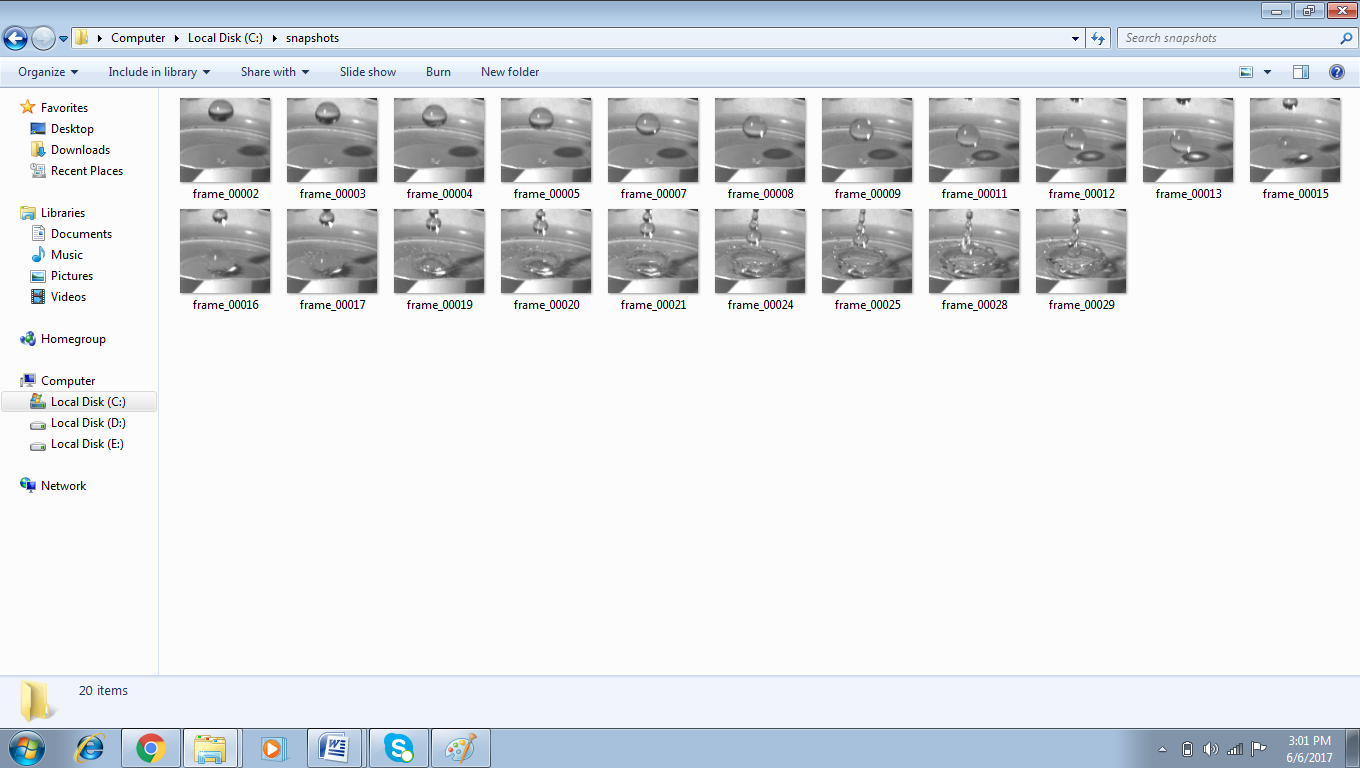


**Figure 5.1:** Video partition- Image frames

**Step 2: Key Frame selection**

Input: Using mean and standard deviation

Output: Only 20 image frames are selected for data embedding.



**Figure 5.2:** Key frame selection

Step 3: Reserve room for data embedding

Input: 20 key frames

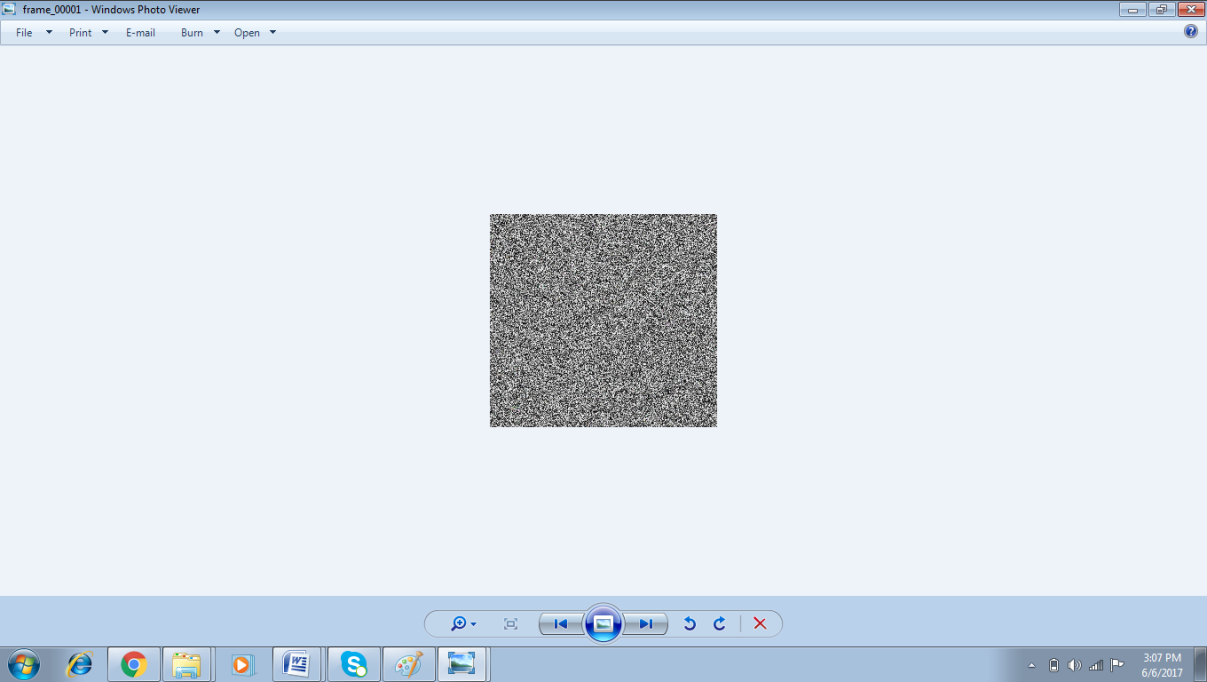
Output: 

**Figure 5.3:** Reserve Room Before Encryption (RRBE)

Step 4: Image Encryption

Input: 

**Figure 5.4:** Image frame before encryption

Output: 

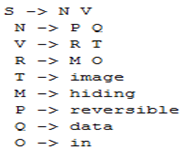
**Figure 5.5:** Image Encryption using RSA algorithm

* 1. **Data Hiding In Encrypted Image**

Step 1: Context free grammar generation

Input: Text message. Example “reversible data hiding in image”

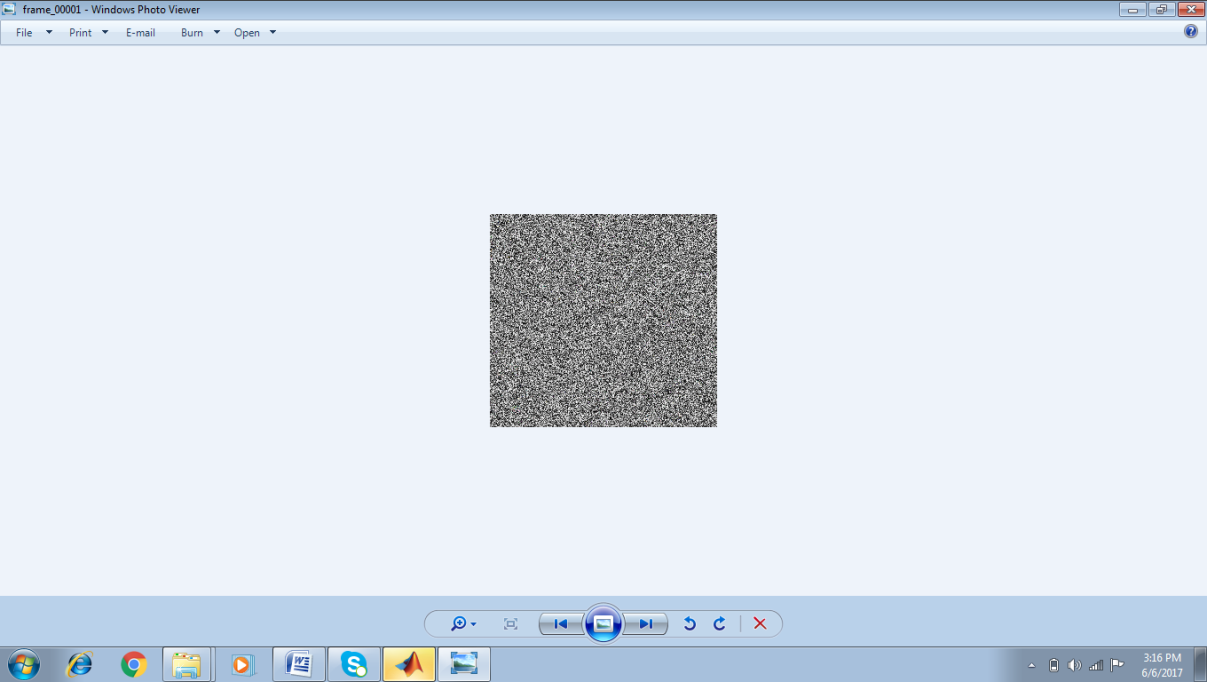
Output:



**Figure 5.6:** CFG for input text

Step 2: Data Hiding

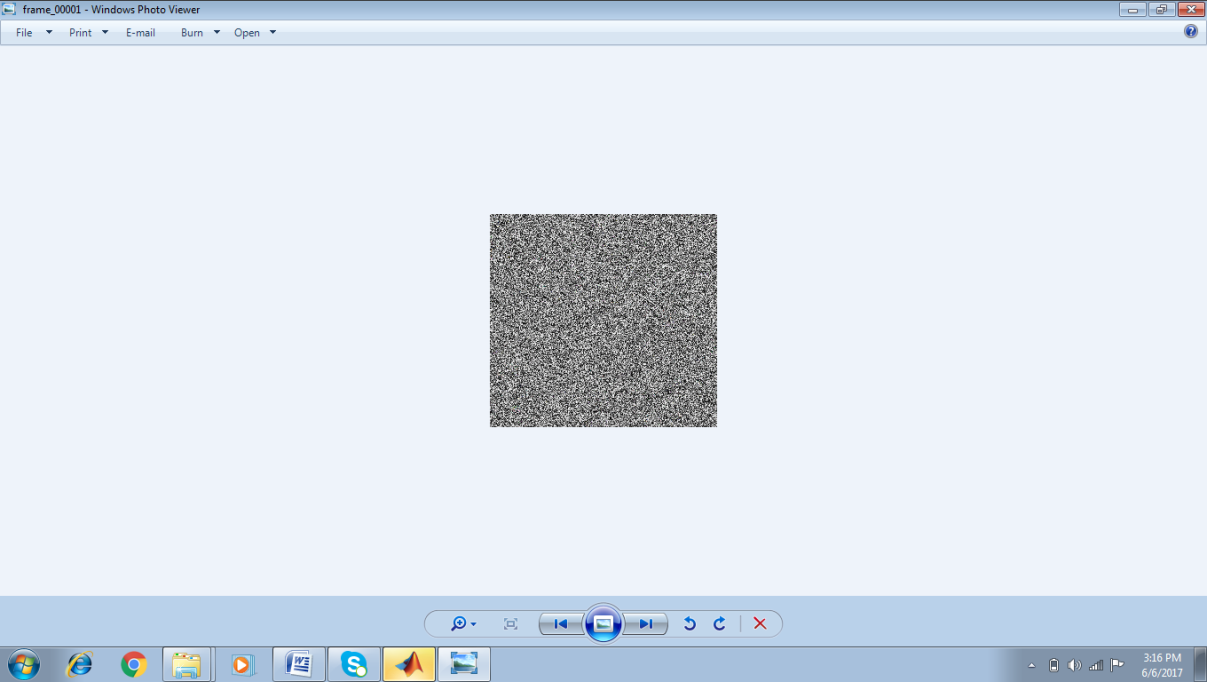
Input: Encrypted image and text file

Output:

**Figure 5.7:** Data embedded in encrypted image

* 1. **Data Extraction And Video Recovery**

Step 1: Data Extraction

Input : 

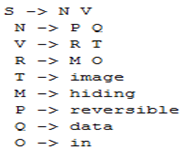
**Figure 5.8:** Data embedded in encrypted image

Output: S -> N V

Step 2: Merging text files

Input: Data extracted from multiple key frames

Output:



**Figure 5.8:** CFG extracted from encrypted images

Step 3: CFG parsing

Input: CFG production rules

Output :



**Figure 5.10:** Parsing CFG

Step 4: Image decryption

Input: Encrypted Image and Private Key

Output:



**Figure 5.11: Image decryption**

* 1. **Summary**

The detailed implementation in matlab was given. Data extraction and image recovery was obtained without any error.

**Chapter 6**

**Conclusion and Future Work**

* 1. **Conclusion**

A proposal for developing a reversible data hiding for encrypted video using context free grammar was suggested. Various technical papers were briefly described that suggested relevant methods to perform reversible data hiding in encrypted image. The detailed design along with the algorithms to be performed at each step of the implementation was explicitly stated. The implementation of the RDH system in matlab was shown. The security of the data is much more increased due to the use of context free grammar.

* 1. **Future Work**

The work presented in this project is, hopefully, comprehended within the defined scope, but research never ends, therefore, future research is expected to explore horizons beyond the scope of this project.

In future, different reversible data hiding techniques can be used for data embedding such as difference expansion, histogram shifting, DWT etc

**Bibliography**

1. Gayatri Pisal, Aparna More, Sonali Pawar, and Ashwini Vishwakarma “Separable Reversible Data Hiding in Encrypted Video File IJRCS - International Journal of Research in Computer Science, Volume: 02 Issue: 04 2015.
2. Mr. Ratnakar Kumbhar, Mr. Sagar Yamgar, Ms. Rupali Ghule, Prof. Murkute P.K “Data Hiding in Encrypted H.264/AVC Video Streams By Codeword Substitution” IEEE International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 3, Issue 2, pp: (323-331), Month: April - June 2015
3. T. Margaret, “Reversible Data Hiding In Encrypted Images by XOR Ciphering Technique”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering , Vol. 3, Issue 2, February 2014
4. Chinju K Sunil, Prathibha Varghese, “A SECURED DATA TRANSMISSION SYSTEM BY REVERSIBLE DATA HIDING WITH SCALABLE COMPRESSION,” INTERNATIONAL JOURNAL OF ELECTRONICS AND COMMUNICATION ENGINEERING & TECHNOLOGY (IJECET), Volume 5, Issue 12, December (2014), pp. 84-92
5. Jewel Vincent Chittilappilly, Tressa Micheal,” Reversible Data Hiding in Encrypted Images using Rhombus Method by RRBE”, IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 5, Ver. II (Sep - Oct .2015), PP 01-07
6. Nilesh Solanki, Mahesh Parmar, Dr. Vineet Richhariya “Non-Saperable Reversible Data Hiding in Encrypted Image Using Chaoutic Map”, International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1656-1659
7. Zhenxing Qian, Xinpeng Zhang, “ reversible data hiding in encrypted images using distributed source encoding”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY
8. Lincy Rachel Mathews, Arathy C. Haran V., “Histogram Shifting Based Reversible Data Hiding,” International Journal of Engineering Trends and Technology (IJETT) – Volume 10 Number 10 - Apr 2014
9. Zhenxing Qian, Xinpeng Zhang, Guorui Feng “Reversible Data Hiding in Encrypted Images Based on Progressive Recovery” IEEE Signal Processing Letters (Volume: PP, 28 June 2016)
10. Akira Nishimura, “Reversible audio data hiding using linear prediction and error expansion,” 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing
11. Shijun Xiang and Zihao Li, “Reversible audio data hiding algorithm using noncausal prediction of alterable orders” DOI 10.1186/s13636-017-0101-9, Xiang and Li EURASIP Journal on Audio, Speech, and Music Processing (2017) 2017:4
12. Lixiao Zheng, Duanyi Wu, “A Sentence Generation Algorithm for Testing Grammars”, 2009 33rd Annual IEEE International Computer Software and Applications Conference
13. J. Kieffer and E-h. Yang, “Design of context-free grammars for lossless data compression,”Technical Report, Dept. of Electrical & Computer Engineering, University of Minnesota Twin Cities.

**Publications**

1. Presented and Published a Paper on “Reversible data hiding in encrypted video using context free grammar” at CSIR Sponsored National Conference on Advances in Computational Biology, Communication, and Data Analytics, ACBCDA2017, May 13, 2017, Jain College of Engineering, Belagavi, India.
2. Received an Acceptance Notification to Present and Publish a Paper on “Reversible data hiding using context free grammar” at the International Conference on Ubiquitous Computing (ICUC-17), organized by Sinhgad College of Engineering, Pune, Maharashtra on 19th -20th June 2016.

**Plagiarism Report**

From: Gopakumar V <[librarian@unigoa.ac.in](mailto:librarian@unigoa.ac.in)>  
Date: Fri, Jun 9, 2017 at 1:39 PM  
Subject: Fwd: [Urkund] 9% similarity - [librarian@unigoa.ac.in](mailto:librarian@unigoa.ac.in)

Student message: Thesis of Ms. Samiksha Velip           
  
Document: ME\_CSE\_thesis\_Samiksha\_2017.docx [D29284106]  
  
  
About 9% of this document consists of text similar to text found in 55 sources. The largest marking is 64 words long and is 94% similar to its primary source.  
  
PLEASE NOTE that the above figures do not automatically mean that there is plagiarism in the document. There may be good reasons as to why parts of a text also appear in other sources. For a reasonable suspicion of academic dishonesty to present itself, the analysis, possibly found sources and the original document need to be examined closely.